



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 3 年 1 0 月 1 6 日

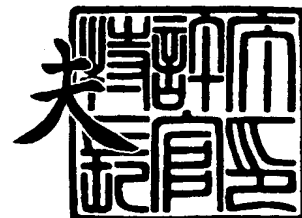
出 願 番 号  
Application Number: 特 願 2 0 0 3 - 3 5 6 7 9 1  
[ST. 10/C]: [ J P 2 0 0 3 - 3 5 6 7 9 1 ]

出 願 人  
Applicant(s): 日 本 ビ ク タ ー 株 式 有 限 公 司

2 0 0 4 年 1 月 2 2 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 0 1 7 4 7



【書類名】 特許願  
【整理番号】 415001084  
【提出日】 平成15年10月16日  
【あて先】 特許庁長官 殿  
【国際特許分類】 H04N 1/387  
G09C 5/00  
H04N 1/41  
G06F 15/66

【発明者】  
【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 日本ビクター株  
式会社内  
【氏名】 上田 健二郎

【発明者】  
【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 日本ビクター株  
式会社内  
【氏名】 西谷 勝義

【発明者】  
【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 日本ビクター株  
式会社内  
【氏名】 菅原 隆幸

【特許出願人】  
【識別番号】 000004329  
【氏名又は名称】 日本ビクター株式会社  
【代表者】 寺田 雅彦

【代理人】  
【識別番号】 100089956  
【弁理士】  
【氏名又は名称】 永井 利和  
【電話番号】 045(913)2980

【先の出願に基づく優先権主張】  
【出願番号】 特願2003- 93383  
【出願日】 平成15年 3月31日

【手数料の表示】  
【予納台帳番号】 004813  
【納付金額】 21,000円

【提出物件の目録】  
【物件名】 特許請求の範囲 1  
【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【包括委任状番号】 9200897

**【書類名】 特許請求の範囲****【請求項 1】**

ディジタル画像データに対して秘匿的操作処理を施した後に直交変換を含む符号化処理を行って符号化信号を得るデータ処理装置であって、

前記ディジタル画像データの各画素の輝度データを前記符号化処理のデータ処理単位に相当する所定ブロック単位で記憶する記憶手段と、

前記記憶手段が記憶した前記所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求める代表値演算手段と、

前記代表値演算手段が求めた代表値が予め設定した値： $N$ （但し、 $N$ は2以上の整数）の倍数である場合には前記記憶手段の各輝度データをそのままとし、前記 $N$ の倍数以外の場合には、前記代表値が前記 $N$ の倍数になるように、前記記憶手段が記憶した各画素の輝度データを最小の諧調変更幅となる条件で書き換えるデータ書き換え手段と、

前記代表値演算手段と前記データ書き換え手段による秘匿的な画像データ処理が完了する度に、前記記憶手段に対するデータの書き込み／読み出し制御を実行する入出力制御手段と、

前記入出力制御手段により読み出された書き換え後の前記ディジタル画像データに対して、直交変換を含む符号化処理を行って符号化信号を得る符号化手段と

を具備したことを特徴とするデータ処理装置。

**【請求項 2】**

ディジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値： $N$ （但し、 $N$ は2以上の整数）の倍数である場合には前記各輝度データをそのままとし、前記 $N$ の倍数以外の場合には、前記代表値が前記 $N$ の倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に前記符号化処理を行ったディジタル画像データを対象として改竄の有無を判定する改竄判定装置であって、

前記符号化処理に対応する復号化手段と、

復号化されたディジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手段と、

前記判定側代表値演算手段が求めた代表値を前記 $N$ で除算する除算手段と、

前記除算手段による除算結果の剰余に0以外の整数が含まれていた場合に、その除算結果に対応する所定ブロックを含む画像領域が改竄されたものと判定する判定手段と

を具備したことを特徴とする改竄判定装置。

**【請求項 3】**

ディジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値： $N$ （但し、 $N$ は2以上の整数）の倍数である場合には前記各輝度データをそのままとし、前記 $N$ の倍数以外の場合には、前記代表値が前記 $N$ の倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に前記符号化処理を行って得られるディジタル画像データを対象として改竄の有無を判定する改竄判定装置であって、

前記符号化処理に対応する復号化手段と、

復号化されたディジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手段と、

前記判定側代表値演算手段が求めた代表値を前記 $N$ で除算する除算手段と、

前記除算手段による除算結果の剰余を記憶する判定側記憶手段と、  
所定サイズの画像領域に対応する前記判定側記憶手段の各剰余について、0の数:Aと、0以外の整数の数:Bをそれぞれ計数する計数手段と、  
前記計数手段の各計数値に基づいて、 $A/(A+B) \leq Z1$  (但し、Z1は1/Nより大きい設定値) が成立した場合に、前記所定サイズの画像領域の画像データに改竄が施されたものと判定する判定手段と  
を具備したことを特徴とする改竄判定装置。

【請求項4】

デジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値:M (但し、Mは4以上の整数) の倍数である場合には前記各輝度データをそのままとし、前記Mの倍数以外の場合には、前記代表値が前記Mの倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に前記符号化処理を行って得られるデジタル画像データを対象として改竄の有無を判定する改竄判定装置であって、

前記符号化処理に対応する復号化手段と、

復号化されたデジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手段と、

前記判定側代表値演算手段が求めた代表値を前記Mで除算する除算手段と、

前記除算手段による除算結果の剰余を記憶する判定側記憶手段と、

所定サイズの画像領域に対応する前記判定側記憶手段の各剰余について、0の数:Aと、0から前記Mまでの整数値の内の中央値 (但し、前記Mが奇数のときはM/2に最も近い2つの値) の数:Cをそれぞれ計数する計数手段と、

前記計数手段の各計数値に基づいて、 $A/(A+C) \leq Z2$  (但し、Z2は1/Mより大きい設定値) が成立した場合に、前記所定サイズの画像領域の画像データに改竄が施されたものと判定する判定手段と

を具備したことを特徴とする改竄判定装置。

【請求項5】

デジタル画像データに対して秘匿的操作処理を施した後に直交変換を含む符号化処理を行って符号化信号を得るためのデータ処理プログラムであって、

前記デジタル画像データの各画素の輝度データを前記符号化処理のデータ処理単位に相当する所定ブロック単位で記憶手段に書き込むデータ書き込み手順と、

前記記憶手段に書き込まれた前記所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求める代表値演算手順と、

前記代表値演算手順で求めた代表値が予め設定した値:N (但し、Nは2以上の整数) の倍数である場合には前記記憶手段の各輝度データをそのままとし、前記Nの倍数以外の場合には、前記代表値が前記Nの倍数になるように、前記記憶手段が記憶した各画素の輝度データを最小の諧調変更幅となる条件で書き換えるデータ書き換え手順と、

前記代表値演算手順と前記データ書き換え手順による秘匿的な画像データ処理が完了する度に、前記記憶手段に対するデータの書き込み/読み出し制御を実行する入出力制御手順と、

前記入出力制御手順で読み出された書き換え後の前記デジタル画像データに対して、直交変換を含む符号化処理を行って符号化信号を得る符号化手順と

をコンピュータに実行させることを特徴とするデータ処理プログラム。

【請求項6】

デジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の

輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値：N（但し、Nは2以上の整数）の倍数である場合には前記各輝度データをそのままとし、前記Nの倍数以外の場合には、前記代表値が前記Nの倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に前記符号化処理を行って得られるデジタル画像データを対象として改竄の有無を判定する改竄判定プログラムであって、

前記符号化処理に対応する復号化処理を行う復号化手順と、

復号化されたデジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手順と、

前記判定側代表値演算手順で求めた代表値を前記Nで除算する除算手順と、

前記除算手順による除算結果の剰余に0以外の整数が含まれていた場合に、その除算結果に対応する所定ブロックを含む画像領域が改竄されたものと判定する判定手順と

をコンピュータに実行させることを特徴とする改竄判定プログラム。

#### 【請求項7】

デジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値：N（但し、Nは2以上の整数）の倍数である場合には前記各輝度データをそのままとし、前記Nの倍数以外の場合には、前記代表値が前記Nの倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に前記符号化処理を行って得られるデジタル画像データを対象として改竄の有無を判定する改竄判定プログラムであって、

前記符号化処理に対応する復号化処理を行う復号化手順と、

復号化されたデジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手順と、

前記判定側代表値演算手順で求めた代表値を前記Nで除算する除算手順と、

前記除算手順による除算結果の剰余をコンピュータの記憶手段に記憶させる記憶手順と

、  
所定サイズの画像領域に対応する前記記憶手段の各剰余について、0の数：Aと、0以外の整数の数：Bをそれぞれ計数する計数手順と、

前記計数手順で求めた各計数値に基づいて、 $A / (A + B) \leq Z1$ （但し、Z1は $1 / N$ より大きい設定値）が成立した場合に、前記所定画像領域の画像データが改竄されたものと判定する判定手順と

をコンピュータに実行させることを特徴とする改竄判定プログラム。

#### 【請求項8】

デジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値：M（但し、Mは2以上の整数）の倍数である場合には前記各輝度データをそのままとし、前記Mの倍数以外の場合には、前記代表値が前記Mの倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に前記符号化処理を行って得られるデジタル画像データを対象として改竄の有無を判定する改竄判定プログラムであって、

前記符号化処理に対応する復号化処理を行う復号化手順と、

復号化されたデジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手順と、

前記判定側代表値演算手順で求めた代表値を前記Mで除算する除算手順と、

前記除算手順による除算結果の剰余をコンピュータの記憶手段に記憶させる記憶手順と

、  
所定サイズの画像領域に対応する前記記憶手段の各剰余について、0 の数: A と、0 から前記 M までの整数値の内の中央値（但し、前記 M が奇数のときは  $M/2$  に最も近い 2 つ値）となった場合の数: C をそれぞれ計数する計数手順と、

前記計数手順で求めた各計数値に基づいて、 $A/(A+C) \leq Z2$ （但し、Z2 は  $1/M$  より大きい設定値）が成立した場合に、前記所定画像領域の画像データが改竄されたものと判定する判定手順と

をコンピュータに実行させることを特徴とする改竄判定プログラム。

## 【書類名】明細書

【発明の名称】データ処理装置及び改竄判定装置並びにデータ処理プログラム及び改竄判定プログラム

## 【技術分野】

## 【0001】

本発明はデータ処理装置及び改竄判定装置並びにデータ処理プログラム及び改竄判定プログラムに係り、デジタル画像データに対する直交変換を含む符号化処理を行う前に画像データに対して秘匿的操作処理を行った場合にも、正確な改竄判定を可能にするための装置及びプログラムに関する。

## 【背景技術】

## 【0002】

近年、画像や音楽等のデジタル・コンテンツの流通が益々盛んになり、各種パッケージメディアによる提供だけでなく、インターネット等の通信回線を介した提供方式が採用されることが多くなっている。

従って、流通経路においてデジタル・コンテンツに対して不正な改竄がなされてしまう可能性が高くなり、改竄の有無を検出・判定するための各種の提案がなされている。

## 【0003】

そして、従来からの改竄検出のための最も一般的手法としては、ハッシュ関数を用いたデジタル認証方法が採用されており、特許文献1、2、3等はその応用例である。

このハッシュ関数とは、長いデータを攪乱して一定の長さ（例えば、128ビット）のハッシュ値に圧縮する操作関数であり、関数値： $y$  が与えられたときに、 $y = h_K(x)$  となる  $x$  を求めることが困難な一方向性関数： $h_K$  である。

改竄検出にハッシュ関数を利用する場合には、 $x$  がデータ（任意の長さ）で、 $y$  が前記のように固定長とされ、 $h_K$  は送信者と受信者だけが知っている秘密鍵： $K$  によって変化するものとされる。

このデジタル認証方法では、送信者がデータ： $x$  にハッシュ値： $y$  を添付して受信者側へ送る。但し、万全を期する場合にはデータ： $x$  とハッシュ値： $y$  が暗号化されることもある。

受信者側では、前記の秘密鍵： $K$  を用いてハッシュ値を計算し、その計算結果が受信したハッシュ値： $y$  と一致すれば「改竄なし」とされ、不一致の場合には「改竄あり」と判断される。

尚、代表的なハッシュ関数にはMD5（Message Digest 5）やSHA（Secure Hash Algorithm）等があるが、それらは下記の特許文献1に詳しく解説されている。

## 【0004】

【特許文献1】特開平11-196392号公報

【特許文献2】特開2001-122861号公報

【特許文献3】特開2002-016596号公報

【非特許文献1】岡本栄司著 「暗号理論入門」 共立出版株式会社

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【0005】

ところで、一般に画像データはデータサイズが非常に大きくなるため、JPEG（Joint Photographic Experts Group）やMPEG（Moving Picture Experts Group）等の直交変換を含む非可逆圧縮処理を施して提供されることが多い。

特に、通信回線を介して提供する場合には、伝送時間を短縮するために、圧縮率が高い前記のような非可逆圧縮処理を行うのが通例である。

一方、前記のハッシュ関数によるデジタル認証方法では、データについて1ビットでも変更があれば「改竄有り」と判定する。

## 【0006】

従って、前記のデジタル認証方式において、画像データの圧縮処理前に改竄判定のた

めの情報を付加すると、圧縮処理後に多くのビットが変化して改竄判定が不可能になるため、常に圧縮処理が完了した後にその情報を付加しなければならない。

また、改竄判定のための情報を一旦付加すると、その後に画像データを再加工することはできなくなる。

これは、画像データの提供者に不利・不便を強いることになり、画像データの取扱いとその流通に関して大きな障害となる。

#### 【0007】

そこで、本発明は、画像データの符号化圧縮前に改竄判定のための情報を付加しても、本来の改竄のみを正確に判定することが可能なシステムを提供することを目的として創作された。

#### 【課題を解決するための手段】

#### 【0008】

本発明は、デジタル画像データに対して秘匿的操作処理を施した後に直交変換を含む符号化処理を行って符号化信号を得るデータ処理装置と、そのデータ処理装置で操作された画像データを復号化して改竄判定を行う改竄判定装置、及びそれら装置をコンピュータで構成する場合に適用されるプログラムに関するものである。

#### 【0009】

先ず、データ処理装置は、デジタル画像データの各画素の輝度データを前記符号化処理のデータ処理単位に相当する所定ブロック単位で記憶する記憶手段と、前記記憶手段が記憶した前記所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求める代表値演算手段と、前記代表値演算手段が求めた代表値が予め設定した値：N（但し、Nは2以上の整数）の倍数である場合には前記記憶手段の各輝度データをそのままとし、前記Nの倍数以外の場合には、前記代表値が前記Nの倍数になるように、前記記憶手段が記憶した各画素の輝度データを最小の諧調変更幅となる条件で書き換えるデータ書き換え手段と、前記代表値演算手段と前記データ書き換え手段による秘匿的な画像データ処理が完了する度に、前記記憶手段に対するデータの書き込み／読み出し制御を実行する入出力制御手段と、前記入出力制御手段により読み出された書き換え後の前記デジタル画像データに対して、直交変換を含む符号化処理を行って符号化信号を得る符号化手段とを具備したことを特徴とするものである。

#### 【0010】

このデータ処理装置では、符号化処理である所定ブロック単位でデジタル画像データに対する秘匿的操作処理を行い、代表値演算手段で求めた所定ブロックの各画素の輝度データに係る代表値を設定値：Nの整数倍とするように、データ書き換え手段によって各輝度データを書き換える。

ここに、代表値を求めるための量子化機能を持つ所定関数としては、前記所定ブロックの各画素の輝度データを変数とするものであり、輝度データの平均値やメジアンを演算して四捨五入化整数値を求めるような関数が典型例であるが、それらに限定されず、四捨五入化する前の演算には多種多用な関数を適用できる。

また、前記書き換えを行う場合に、各画素の輝度データを最小の諧調変更幅となる条件で行うのは、画像自体の変化を可能な限り小さく抑制するためである。

いずれにしても、書き換え操作後の画像データは、各所定ブロックの前記代表値がNの整数倍となり、その意味での規則性を具有することになる。

そして、このデータ処理装置では、前記書き換え操作後の画像データに対して直交変換を含む符号化処理を行う。

その場合、直交変換を含む符号化処理においては、画像データを前記の所定ブロック単位で直交変換を行って量子化するが、AC成分についてはその冗長度が削減されるものの、DC成分（即ち、前記所定ブロックの輝度平均値）はほぼそのまま保存される。

従って、前記の規則性は保存されることになり、画像データの流過程においても改竄がなされていればその規則性が損壊することから、それを改竄判定に用いることができ



る。

#### 【0011】

本発明の改竄判定装置は、次のような構成からなる。

先ず、第1の改竄判定装置は、デジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値：N（但し、Nは2以上の整数）の倍数である場合には前記各輝度データをそのままとし、前記Nの倍数以外の場合には、前記代表値が前記Nの倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に前記符号化処理を行ったデジタル画像データを対象として改竄の有無を判定する改竄判定装置であって、前記符号化処理に対応する復号化手段と、復号化されたデジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手段と、前記判定側代表値演算手段が求めた代表値を前記Nで除算する除算手段と、前記除算手段による除算結果の剰余に0以外の整数が含まれていた場合に、その除算結果に対応する所定ブロックを含む画像領域が改竄されたものと判定する判定手段とを具備したことを特徴とするものである。

#### 【0012】

この第1の改竄判定装置では、先ず、データ処理装置側で処理されたデジタル画像データを復号化し、判定側代表値演算手段によってデータ処理装置側と同様の手順で所定ブロック単位の代表値を求める。

その場合、データ処理装置側の符号化手段とこの改竄判定装置の復号化手段が理想的なものであり、画像データに対して改竄がなされていないとすれば、データ処理装置側で付与された代表値の規則性はそのまま保存されている。

一方、改竄がなされていると、その改竄領域の前記所定ブロックの輝度平均値が変化し、その所定ブロックに係る代表値の規則性が損なわれることになる。

そこで、この改竄判定装置では、除算手段によって判定側代表値演算手段で求めた各所定ブロックに係る代表値をデータ処理装置側での設定値：Nで除算する。

この除算において、もし改竄がなされていないとすれば、除算結果の全ての剰余が0になる筈であり、逆に、改竄があればその剰余の中に1乃至N-1の整数が含まれる筈である。

判定手段はそれを確認し、除算結果の剰余に0以外の整数が含まれていれば、改竄判定ありと判定する。

#### 【0013】

この発明の第2の改竄判定装置は、復号化手段と判定側代表値演算手段と除算手段については第1の改竄判定装置と同様であるが、前記除算手段による除算結果の剰余を記憶する判定側記憶手段と、所定サイズの画像領域に対応する前記判定側記憶手段の各剰余について、0の数：Aと、0以外の整数の数：Bをそれぞれ計数する計数手段とを設け、更に、判定手段が $A / (A + B) \leq Z1$ （但し、Z1は $1 / N$ より大きい設定値）が成立した場合に、前記所定サイズの画像領域の画像データに改竄が施されたものと判定する手段として構成されている点に特徴がある。

#### 【0014】

前記の第1の改竄判定装置では、データ処理装置側での符号化処理及び改竄判定装置側での復号化処理においても各所定ブロックの輝度平均値が変化せず、各所定ブロックの代表値に関する規則性が完全に保存されていることを前提として改竄判定を行うようになっている。

しかしながら、データ処理装置側に適用されている符号化手段や改竄判定装置側に適用されている復号化手段の特性によってはDC成分が変化し、結果的に前記の規則性が失われてしまうことがある。

従って、その場合には本来の改竄がなされていなくても、前記の符号化・復号化段階で

規則性の損壊が僅かに生じ、第1の改竄判定装置のような判定基準ではそれを改竄と判定してしまうことになる。

一方、前記の符号化・復号化段階で規則性の損壊は、画像データの内容によって異なるが、比較的一様に生じる傾向がある。

そこで、この第2の改竄判定装置では、除算手段による除算結果の剰余を判定側記憶手段に一旦記憶させ、剰余の出現状態を統計的に処理して改竄判定を行っている。

即ち、判定側記憶手段が記憶した各剰余に対して所定サイズの画像領域が設定された場合に、計数手段によって剰余が0となった所定ブロックの数: Aと剰余が0以外の整数となった所定ブロックの数: Bを求め、判定手段が統計式:  $A / (A + B)$  によって与えられる値と予め設定した閾値: Z1とを比較し、 $A / (A + B) \leq Z1$ であれば改竄ありと判定する。

ここに、Z1は  $1 / N$  より大きい設定値とされるが、その  $1 / N$  は前記のデータ処理装置による処理を受けていない一般的な画像データを対象とした場合に  $A / (A + B)$  がとる平均的な値である。

そして、この第2の改竄判定装置の判定基準が前記のように統計的処理に基づくものであると共に、符号化・復号化手段の特性を考慮するものであることから、具体的に設定されるZ1の値は、少なくとも、予想される改竄領域の大きさと判定対象とされる画像領域のサイズとの相対的關係及び前記の符号化・復号化手段の特性をパラメータとして決定される。

#### 【0015】

この発明の第3の改竄判定装置は、デジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値: M (但し、Mは4以上の整数) の倍数である場合には前記各輝度データをそのままとし、前記Mの倍数以外の場合には、前記代表値が前記Mの倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に前記符号化処理を行って得られるデジタル画像データを対象として改竄の有無を判定する改竄判定装置であって、前記符号化処理に対応する復号化手段と、復号化されたデジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手段と、前記判定側代表値演算手段が求めた代表値を前記Mで除算する除算手段と、前記除算手段による除算結果の剰余を記憶する判定側記憶手段と、所定サイズの画像領域に対応する前記判定側記憶手段の各剰余について、0の数: Aと、0から前記Mまでの整数値の内の中央値 (但し、前記Mが奇数のときは  $M / 2$  に最も近い2つの値) の数: Cをそれぞれ計数する計数手段と、前記計数手段の各計数値に基づいて、 $A / (A + C) \leq Z2$  (但し、Z2は  $1 / M$  より大きい設定値) が成立した場合に、前記所定サイズの画像領域の画像データに改竄が施されたものと判定する判定手段とを具備したことを特徴とするものである。

#### 【0016】

この第3の改竄判定装置における第2の改竄判定装置と異なる点は、データ処理装置側で設定されているNの値が4以上の値であるMとされており、また第2の改竄判定装置が判定側記憶手段の各剰余について0の数: Aと0以外の整数の数: Bと判定基準に用いたのに対して、0の数: Aと0から前記Mまでの整数値の内の中央値の数: Cとを用いて、判定手段が  $A / (A + C) \leq Z2$  (但し、Z2は  $1 / M$  より大きい設定値) の判定基準を適用していることにある。

データ処理装置側で付与した規則性は、本来の改竄が行われた場合には非常に大きく損壊するが、符号化・復号化過程を経ることによる損壊の度合いは遥かに小さい。

従って、前記の中央値の出現には、符号化・復号化段階での誤差が殆ど反映されず、本来の改竄による影響であることが多い。

その結果、この第3の改竄判定装置の判定基準によれば、第2の改竄判定装置の場合よ

りも厳格な基準を設定でき、Z2をZ1よりも小さな値に設定して本来の改竄だけを誤りなく判定できることになる。

#### 【0017】

以上のデータ処理装置及び改竄判定装置の各手段はコンピュータによって実行させることもでき、その場合には各装置に次のようなプログラムが適用される。データ処理装置側には、前記デジタル画像データの各画素の輝度データを前記符号化処理のデータ処理単位に相当する所定ブロック単位で記憶手段に書き込むデータ書き込み手順と、前記記憶手段に書き込まれた前記所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求める代表値演算手順と、前記代表値演算手順で求めた代表値が予め設定した値：N（但し、Nは2以上の整数）の倍数である場合には前記記憶手段の各輝度データをそのままとし、前記Nの倍数以外の場合には、前記代表値が前記Nの倍数になるように、前記記憶手段が記憶した各画素の輝度データを最小の諧調変更幅となる条件で書き換えるデータ書き換え手順と、前記代表値演算手順と前記データ書き換え手順による秘匿的な画像データ処理が完了する度に、前記記憶手段に対するデータの書き込み／読み出し制御を実行する入出力制御手順と、前記入出力制御手順で読み出された書き換え後の前記デジタル画像データに対して、直交変換を含む符号化処理を行って符号化信号を得る符号化手順とをコンピュータに実行させるデータ処理プログラムが適用される。

#### 【0018】

一方、前記の第1の改竄判定装置に対応するプログラムとしては、デジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値：N（但し、Nは2以上の整数）の倍数である場合には前記各輝度データをそのままとし、前記Nの倍数以外の場合には、前記代表値が前記Nの倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に前記符号化処理を行って得られるデジタル画像データを対象として改竄の有無を判定する改竄判定プログラムであって、データ処理装置側での符号化処理に対応する復号化処理を行う復号化手順と、復号化されたデジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手順と、前記判定側代表値演算手順で求めた代表値を前記Nで除算する除算手順と、前記除算手順による除算結果の剰余に0以外の整数が含まれていた場合に、その除算結果に対応する所定ブロックを含む画像領域が改竄されたものと判定する判定手順とをコンピュータに実行させるプログラムが適用される。

また、前記の第2の改竄判定装置に対応するプログラムとしては、復号化手順と判定側代表値演算手順と除算手順については前記プログラムと同様であるが、前記除算手順による除算結果の剰余をコンピュータの記憶手段に記憶させる記憶手順と、所定サイズの画像領域に対応する前記記憶手段の各剰余について、0の数：Aと、0以外の整数の数：Bをそれぞれ計数する計数手順と、前記計数手順で求めた各計数値に基づいて、 $A / (A + B) \leq Z1$ （但し、Z1は1/Nより大きい設定値）が成立した場合に、前記所定画像領域の画像データが改竄されたものと判定する判定手順とをコンピュータに実行させる改竄判定プログラムが適用される。

また、前記の第3の改竄判定装置に対応するプログラムとしては、デジタル画像データに対する秘匿的操作処理が、直交変換を含む符号化処理単位に相当する所定ブロックの各画素の輝度データを変数とする所定関数を用いて、前記各画素の輝度データに係る代表値を量子化整数値として求め、その代表値が予め設定した値：M（但し、Mは2以上の整数）の倍数である場合には前記各輝度データをそのままとし、前記Mの倍数以外の場合には、前記代表値が前記Mの倍数になるように、前記各輝度データを最小の諧調変更幅となる条件で書き換えるという方法によって施されており、前記秘匿的操作処理を施した後に

前記符号化処理を行って得られるデジタル画像データを対象として改竄の有無を判定する改竄判定プログラムであって、前記符号化処理に対応する復号化処理を行う復号化手順と、復号化されたデジタル画像データに係る前記所定ブロックの各画素の輝度データを前記所定関数の変数として、前記所定ブロックの各画素の輝度データに係る代表値を量子化整数値として求める判定側代表値演算手順と、前記判定側代表値演算手順で求めた代表値を前記Mで除算する除算手順と、前記除算手順による除算結果の剰余をコンピュータの記憶手段に記憶させる記憶手順と、所定サイズの画像領域に対応する前記記憶手段の各剰余について、0の数:Aと、0から前記Mまでの整数値の内の中央値（但し、前記Mが奇数のときは $M/2$ に最も近い2つ値）となった場合の数:Cをそれぞれ計数する計数手順と、前記計数手順で求めた各計数値に基づいて、 $A/(A+C) \leq Z2$ （但し、Z2は $1/M$ より大きい設定値）が成立した場合に、前記所定画像領域の画像データが改竄されたものと判定する判定手順とをコンピュータに実行させるプログラムが適用される。

【発明の効果】

【0019】

本発明の「データ処理装置及び改竄判定装置並びにデータ処理プログラム及び改竄判定プログラム」は、以上の構成を有していることにより、次のような効果を奏する。

データ処理装置と第1の改竄判定装置とで構成したシステムによれば、画像データの直交変換を含む符号化・復号化処理が理想的なものであって画像データのDC成分に変化を及ぼさないという条件下で、符号化処理前に秘匿的なデータ操作を行って改竄判定を正確に行うことを可能にする。

データ処理装置と第2又は第3の改竄判定装置とで構成したシステムによれば、画像データの直交変換を含む符号化・復号化処理によってDC成分が変化するような場合においても、改竄判定を高い精度で行うことを可能にする。

従って、前記の各システムによれば、画像データの提供者において改竄判定のための情報を常に符号化後に付与する必要がなくなり、画像データを提供する際の画像データの取扱いが容易になる。

また、各システムは、画像データの1ビットでも変化すれば改竄とみなすような判定基準ではなく、画素ブロック単位で輝度データに係る代表値に与えた規則性が損なわれたか否かを基準とするため、画像コンテンツを実質的に改竄した場合にのみ改竄と判定し、実際面での運用に適した改竄判定システムが実現できる。

前記の各プログラムは、前記のデータ処理装置及び改竄判定装置をそれぞれマイクロコンピュータ回路で構成する場合に、処理及び判定のための動作手順を合理的に実行させる。

【発明を実施するための最良の形態】

【0020】

以下、本発明の「データ処理装置及び改竄判定装置並びにデータ処理プログラム及び改竄判定プログラム」に係る実施形態について図面を用いて詳細に説明する。

【実施形態1】

先ず、図1はデータ処理装置をハードウェアで構成した場合の機能ブロック図を示す。

同図において、1は入力されるデジタル画像データ（静止画像データ）を輝度データと色差データに分離するデータ分離部、2は分離された輝度データを $8 \times 8$ 画素の画素ブロック単位で記憶する画像メモリ、3は画像メモリ2の各画素の輝度平均値を求めて量子化整数値とする平均値演算部、4は平均値演算部4が求めた輝度平均の整数値に基づいて画像メモリ2の各画素の輝度データを書き換える画素輝度書換部、5は画像メモリ2に対する輝度データのリード/ライトを制御するR/W制御部、6はデータ分離部1が分離した色差データと画像メモリ2で処理された後の輝度データを合成するデータ合成部、7はデータ合成部6で合成された後のデジタル画像データをJPEGの非可逆符号化方式で圧縮するエンコーダ部である。

【0021】

このデータ処理装置は、次のような動作によってデジタル画像データを秘匿的に操作

して符号化する。

原画像データは外部からデータ分離部 1 に入力されて輝度データと色差データに分離され、その内の輝度データは R/W 制御部 5 によって前記の画素ブロック単位で画像メモリ 2 に書き込まれる。

この場合、図 1 の左上部分に示すように、画素ブロックの 64 画素分の輝度値を  $L(i)$  [ $i=1\sim 64$ ] とし、ここでは各輝度値:  $L(i)$  は 256 階調で表現されているものとする。

【0022】

画像メモリ 2 への書き込みが完了すると、平均値演算部 3 は各画素の輝度値の平均値:  $L_{av} (= \sum L(i) / 64)$  を求め、その平均値:  $L_{av}$  を四捨五入して整数化した値:  $L_{av}'$  を求める。

次に、画素輝度書換部 4 は前記の輝度平均値に係る整数値:  $L_{av}'$  が偶数であるか奇数であるかを判断し、偶数の場合には、R/W 制御部 5 へ読み出し指示信号を出力する。

そして、その指示信号を受けた R/W 制御部 5 は、画像メモリ 2 を制御して書き込まれている輝度データをそのまま読み出す。

【0023】

一方、前記の整数値:  $L_{av}'$  が奇数である場合には、画像メモリ 2 の各画素の輝度値:  $L(i)$  の書き換えを実行する。

その書き換え操作は、書き換え後における各画素の輝度値の平均値が偶数 ( $L_{av}' + 1$  又は  $L_{av}' - 1$ ) となるように輝度値:  $L(i)$  を増減させるものであり、その増減量 ( $+\Delta p$  又は  $-\Delta m$ ) は最小の諧調変更幅となる条件とされる。

即ち、原画像データができるだけ変化させない条件で各画素の輝度値:  $L(i)$  が書き換えられる。

そして、その書き換えが完了すると、画素輝度書換部 4 が R/W 制御部 5 へ読み出し指示信号を出力し、R/W 制御部 5 によって画像メモリ 2 の各輝度データが読み出される。

【0024】

その結果、画像メモリ 2 から読み出された各画素の輝度値:  $L_e(i)$  [ $i=1\sim 64$ ] の平均値:  $\sum L_e(i) / 64$  は偶数になっている。

従って、前記の一連の操作処理を繰り返すことにより、その段階における輝度データには画素ブロック単位で規則性が付与されたことになる。

【0025】

画像メモリ 2 から読み出された画素ブロックの各輝度データはデータ合成部 6 へ出力され、データ分離部 1 で先に分離されている画素ブロックの色差データと合成され、その合成後の画像データがエンコーダ部 7 へ出力される。

エンコーダ部 7 では入力された画像データを J P E G の非可逆符号化方式で圧縮するが、その圧縮アルゴリズムは次のとおりである。

(1) D C T 演算部 7 a において画素ブロック単位で D C T (Discrete Cosine Transform) 変換を行う。

(2) D C T 変換で得られた D C T 係数を量子化部 7 b が量子化テーブル 7 c を用いて D C 成分と A C 成分を独立に量子化し、それぞれ D C 係数と A C 係数を得る。

(3) 量子化された D C 係数については、エントロピー符号化部 7 d が、直前の画素ブロックの D C 係数を予測値とした差分値をとり、符号化テーブル 7 e を用いてその差分値を符号化する。一方、量子化された A C 係数については高周波においてゼロとなる係数が多い。ため、エントロピー符号化部 7 d は、A C 係数を周波数成分の低い方から高い方へ画素ブロック内で並べ替えてジグザグ・スキャンを行い、符号化テーブル 7 e を用いてゼロ係数の連続長とそれを終端する非ゼロ係数の値との組み合わせデータとして符号化する。

【0026】

そして、符号化された圧縮画像データは、一旦何等かの記憶手段に格納され、それを記憶媒体に記録して提供されるか、又は通信回線を介して提供先へ配信されることになる。

この場合、A C 成分は符号化によって変化しているが、D C 成分は殆ど変化せず、画素ブロック単位で輝度平均値:  $\sum L_e(i) / 64$  は偶数であるという規則性はそのまま保存さ

れていると想定できる。

即ち、輝度データはDCT変換において低周波項に集中し、主に高周波成分の冗長性を除去する前記の圧縮処理では画素ブロック単位の輝度平均値に影響しない。

#### 【0027】

ところで、前記の圧縮画像データは提供先で再生されるが、記憶媒体の流通経路やネットワーク上で改竄されている可能性がある。

その改竄の有無は、次のような改竄判定装置によって判定される。

先ず、図2は改竄判定装置をハードウェアで構成した場合の機能ブロック図を示す。

同図において、21は入力された圧縮画像データを復号するデコーダ部、22は復号された画像データから輝度データだけを分離する輝度データ分離部、23は分離された輝度データを $8 \times 8$ 画素の画素ブロック単位で記憶する画像メモリ、24は画像メモリ23の各画素の輝度平均値を求めて量子化整数値とする平均値演算部、25は平均値演算部24が求めた輝度平均値（整数値）を「2」で除算する除算部、26は画像メモリ2に対して輝度データを画素ブロック単位で更新する書込制御部、27は除算部25による画素ブロック毎の除算結果の剰余に基づいて改竄がなされているか否かを判定する改竄判定部、28は改竄判定部28の判定結果を表示する表示部である。

#### 【0028】

この改竄判定装置では、先ず、デコーダ部21で圧縮画像データに対して前記のデータ処理装置側のエンコーダ部7と逆の処理を施して復号化するが、その復号アルゴリズムは次のとおりである。

- (1) エントロピー復号化部21aが復号化テーブル21bを用いて圧縮画像データを量子化インデックスに戻す。
- (2) 逆量子化部21cが逆量子化テーブル21dを用いて量子化インデックスを逆量子化する。
- (3) 逆DCT係数演算部21eで逆量子化されたDCT係数を復号画像データに再構成する。

#### 【0029】

次に、復号された画像データは輝度データ分離部22によって輝度データだけが分離される。

その場合、前記のデータ処理装置側から提供された記憶媒体の流通経路やネットワーク上で画像データが改竄されていなければ、分離された輝度データはデータ処理装置側の画像メモリ2から読み出されたデータと同一であり、画素ブロック単位で輝度平均値： $\sum Le(i)/64$ が偶数であるという規則性を有しているが、もし改竄がなされていればその規則性は損なわれている。

ここでは、改竄の有無が不明であるとして、図2の中央に示すように、画素ブロックの64画素分の輝度値を $Le(i)x [i=1 \sim 64]$ として表す。

#### 【0030】

分離された輝度データは、書込制御部26の制御によって画素ブロック単位で画像メモリ23に書き込まれる。

そして、平均値演算部24が、前記のデータ処理部側の平均値演算部3と同様に、各画素の輝度値： $Le(i)x [i=1 \sim 64]$ の平均値： $L_{avx} (= \sum Le(i)x / 64)$ を求め、その平均値： $L_{avx}$ を四捨五入して整数化した値： $L_{avx}'$ を求める。

#### 【0031】

次に、除算部25が前記の整数化された平均値： $L_{avx}'$ を2で除算する。

その場合、画像データに対して改竄がなされていなければ、前記のように画素ブロックは輝度平均値： $\sum Le(i)/64$ が偶数であるという規則性を有しているため、除算結果の剰余は「0」になる。

一方、もし改竄がなされており、画素ブロックがその改竄領域に含まれるものであれば、除算結果の剰余は「1」になる。

#### 【0032】

そこで、改竄判定部 27 は、除算部 25 が求めた除算結果の剰余を内蔵メモリに順次セーブしてゆく。

そして、改竄判定部 27 は剰余値のセーブを行う度に書込制御部 26 へ制御信号を出力し、書込制御部 26 が上書き方式で次の画素ブロックの輝度データを画像メモリ 23 へ書き込み、平均値演算部 24 と除算部 25 と改竄判定部 27 が前記の手順を繰り返す。

このようにして、検査対象とされる画像データについての処理が完了すると、改竄判定部 27 は内蔵メモリにセーブさせた各剰余を確認し、もし剰余に「1」が含まれていればその画像データについて「改竄あり」と判定し、逆に「1」が含まれていなければ「改竄なし」と判定する。

例えば、内蔵メモリ上で各画素ブロック単位での除算結果の剰余が図 3 に示すような結果として得られた場合には、剰余「1」を含んでいるために改竄がなされていると判定される。

#### 【0033】

また、図 3 に示す各剰余は各画素ブロックに対応しているため、デコーダ部 21 が出力する復号化後の画像データを表示部 28 で表示させておき、改竄がなされた領域を表示画面上で具体的に示すことも可能である。

一方、画像データに対する改竄の有無だけを判定するのであれば、改竄判定部 27 は剰余値をセーブしてゆく必要はなく、除算部 25 で剰余「1」が求められた時点で「改竄あり」の判定を行えば足りる。

#### 【0034】

尚、この実施形態では、データ処理装置側で輝度平均値： $\sum Le(i)/64$  が偶数になるように規則性を持たせているが、必ずしも偶数である必要はなく、2 以上の整数の倍数であればよく、その場合には、改竄判定装置側の除算部 25 がその値で除算を行うようにすればよい。

また、この実施形態では、画素ブロックの輝度平均値を求めるようにしているが、平均値演算関数に限らず、輝度データを変数とした各種関数を適用して画素ブロックの代表値を求めるようにしてもよく、その意味で画像データの操作に関して秘匿性を持たせることができる。

#### 【0035】

##### 〔実施形態 2〕

前記の実施形態 1 では、データ処理装置側のエンコーダ部 7 と改竄判定装置側のデコーダ部 21 が理想的な特性を有しており、データ処理装置で各画素ブロックに与えた輝度平均値： $\sum Le(i)/64$  が偶数であるという規則性が全く損なわれないことを前提として改竄判定装置を構成している。

しかしながら、実際のエンコーダとデコーダでの直交変換を含む符号化・復号化処理において DC 成分が変化しない条件で符号化・復号化がなされることはむしろ稀であり、一般的なエンコーダやデコーダでは僅かであるが DC 成分に変化が生じる。

その場合、実施形態 1 のデータ処理装置で画像メモリ 2 から読み出された後の画素ブロックに与えられている規則性は、エンコーダ部 7 での符号化過程で損壊し、また改竄判定装置側での復号化過程でも影響を受けることになる。

従って、改竄判定装置の輝度データ分離部 22 で分離された輝度データは、画像データに改竄がなされていない場合であっても前記の規則性を失っており、改竄がなされている場合には、符号化・復号化過程による要因と改竄による要因が重畳した態様で規則性の喪失が発生していることになる。

但し、符号化・復号化過程での規則性の損壊は、その性質上、それほど多くの画素ブロックに現れるものではなく、画像データの内容によって異なるものの、ほぼ一定の割合で、且つ画像データ全体に対して一様に現れる。

#### 【0036】

そこで、この実施形態では、改竄判定装置の判定処理機能部分を下記のように構成し、符号化・復号化過程で規則性の損壊があっても、本来の改竄のみを正確に判定できるよう

にしている。

但し、前提条件として、実施形態 1 におけるデータ処理装置では画素ブロックの輝度平均値： $L_{av}$  を整数化した値： $L_{av}'$  が 2 の倍数となるように各画素の輝度データを書き換えて規則性を持たせていたが、この実施形態ではデータ処理装置側が 4 の倍数に書き換えて規則性を持たせているものとする。

図 4 はこの実施形態に係る改竄判定装置の機能ブロック図を示す。

同図と図 2 を比較すれば明らかなように、デコーダ部 21、輝度データ分離部 22、画像メモリ 23、平均値演算部 24、除算部 25、及び表示部 28 が設けられていることは実施形態 1 の改竄判定装置と同様であり、また、それらの基本的機能は除算部 25 が除数を「4」に設定していることを除いて同一である。

従って、ここではそれらの機能とデータ処理についての説明は省略する。

#### 【0037】

この実施形態に係る改竄判定装置の特徴は、除算部 25 が求めた除算結果の剰余を格納する剰余メモリ 31 と、剰余メモリ 31 が記憶した各剰余の内で「0」の数とそれ以外の値（「1」、「2」、「3」）の数をカウントする計数部 32 と、剰余メモリ 31 と計数部 32 に対して判定を行うべき画像領域に対応した剰余の格納領域を指定する領域設定部 33 と、計数部 32 によるカウント数を統計的に処理して改竄判定を行う改竄判定部 34 とが設けられている点にある。

#### 【0038】

以下、この実施形態における改竄判定動作について説明する。

先ず、平均値演算部 24 で画素ブロックの輝度平均値： $L_{avx}$  を整数化した値： $L_{avx}'$  を除算部 25 が「4」で除算し、その除算結果の剰余が 1 フレーム分の画像データについて剰余メモリ 31 に格納されたとする。

ここで、領域設定部 33 からフレーム内での特定の画像領域に係る剰余値を指定すると、その指定情報が計数部 32 と改竄判定部 34 へ出力され、計数部 32 は「0」の剰余値とそれ以外の剰余値の数をカウントする。

尚、領域指定に際しては、予め 1 フレーム分の画像データに係る各剰余値を複数に分割しておいて分割領域単位で指定する方式や、デコーダ部 21 から得られる復号後の画像データを表示部 28 に表示させておいて任意の領域を指定する方式が採用できる。

#### 【0039】

そして、改竄判定部 34 では、計数部 32 が求めた「0」の剰余値のカウント数： $A$  とそれ以外の剰余値のカウント数： $B$  を用いて、 $A / (A + B)$  を演算し、その演算結果と予め設定した閾値： $Z1$  とを比較して、 $A / (A + B) \leq Z1$  が成立していれば「改竄あり」と判定し、逆の場合には「改竄なし」と判定する。

#### 【0040】

ところで、前記の閾値： $Z1$  は次のような観点から定められる。

先ず、前記のデータ処理装置のように規則性を与えていない画像データがこの改竄判定装置へ入力された場合には、元々規則性がないために  $A / (A + B)$  の値はほぼ  $1 / 4$  となる。即ち、除算部 25 での除算結果の剰余は「0」、「1」、「2」、「3」がほぼ均等に現れる。

これは、画像データ全体に改竄を施した場合とほぼ同様とみなせ、 $Z1$  は少なくとも  $1 / 4$  以上の範囲で設定されることになる。

#### 【0041】

その上で、符号化・復号化過程での規則性が損なわれる度合いを計測する。

この計測は、前記のデータ処理装置で処理された画像データを用い、改竄を施すことなく、そのままこの改竄判定装置に入力して除算部での除算結果の剰余の現れ方を確認することによって行う。

その場合、データ処理装置側のエンコーダ部 7 とこの改竄判定装置のデコーダ部 21 が一般的な J P E G のエンコーダやデコーダであると、画像データの内容によって若干の誤差はあるが、通常は  $A / (A + B)$  の値が約  $4 / 5$  程度になる。



例えば、図5は前記の条件で実験した結果を示し、剰余メモリ31に格納された剰余には「0」と「1」と「3」が現れるが、 $A/(A+B)$ が0.79となっている。

これは、データ処理装置で符号化前に各画素ブロックに与えた規則性が、符号化・復号化過程において画像データ全体として20%程度損なわれていることを意味する。

尚、剰余に「2」が現れていないのは、符号化・復号化過程では輝度データに与える影響が比較的小さく、剰余が「2」となるような大きな変化が生じていないからである。

従って、画像データのどの領域についても、前記の規則性が損壊した画素ブロックが常に20%前後存在していることを前提としなければならないが、その割合はエンコーダ部7とデコーダ部21の特性によって若干変化する。

#### 【0042】

次に、画像データに対して改竄がなされている場合を仮定する。

まず、改竄が画像上のどの領域に対して如何なる大きさで行われるかは予測できない。

また、この実施形態の改竄判定装置では、画像データに与えた規則性についての損壊の度合いを統計的に計測するため、予想される改竄領域の大きさと改竄判定を行おうとする指定領域のサイズとの相対的關係によって $A/(A+B)$ の値が異なることになる。

従って、前記の相対的關係を考慮して閾値：Z1を変化させる必要がある。

#### 【0043】

以上から、閾値：Z1は、少なくとも、データ処理装置側のエンコーダ部7とこの改竄判定装置のデコーダ部21の特性と、予想される改竄領域の大きさと指定領域のサイズの相対的關係をパラメータとして決定される。

エンコーダ部7とデコーダ部21の特性に関しては前記のように実験的に求めることが可能であり、また、前記の相対的關係については操作者が予想される改竄領域の大きさを考慮して指定領域を設定することから、改竄判定部34では主に前記の特性と指定領域のサイズに基づいて閾値：Z1を決定するようにすればよい。

#### 【0044】

##### 〔実施形態3〕

この実施形態も、前記の実施形態2と同様に、符号化・復号化過程で規則性の損壊があっても本来の改竄のみを正確に判定できるようにする改竄装置に関する。

この実施形態に係る改竄判定装置の機能ブロック図は、実施形態2の装置に係る図4と同様であるが、計数部32と改竄判定部34での処理手順が相違しており、異なった判定基準で改竄判定を行う。

従って、ここでは計数部32と改竄判定部34の動作説明のみに留め、他の機能部分に関する説明を省略する。

#### 【0045】

まず、除算部25が求めた除算結果の剰余が剰余メモリ31に格納され、領域設定部33で領域指定が行われると、計数部32がその領域対応した各剰余の内で「0」の数と「2」の数をそれぞれカウントする。

そして、改竄判定部34では、それらのカウント数をそれぞれAとCとして $A/(A+C)$ を求め、 $A/(A+C) \leq Z2$ が成立していれば「改竄あり」と判定し、逆の場合には「改竄なし」と判定する。

即ち、実施形態2では「0」の数：Aと「0」以外の値の数：Bを求めて $A/(A+B) \leq Z1$ の判定基準を適用したが、この実施形態では、「0」から「4」までの整数値のうちの中央値に相当する「2」のカウント数：Cを用いており、閾値：Z2も閾値：Z1よりも大きい値を用いて改竄の有無を判定する。

#### 【0046】

実施形態2で説明したように、符号化・復号化過程での規則性の損壊によって出現する剰余は「1」と「3」が殆どであり、「2」が出現する確率は極めて小さい。

そして、改竄がなされた場合には、当然に「1」と「3」の剰余が多くなると共に「2」の剰余も多く出現し、それに応じて「0」の剰余は極端に少なくなる。

即ち、改竄による $A/(A+C)$ の値の減少率は、実施形態2の場合の $A/(A+B)$

の値よりも遥かに大きいものとなる。

従って、閾値：Z2を閾値：Z1よりも相当に大きい値（例えば、0.9～0.995）に設定しておき、改竄判定を高い精度で行えることになる。

#### 【0047】

図6は改竄があった場合における剰余の出現状態を示し、点線で囲まれた範囲が改竄のなされた画像領域に相当する。

同図では、図5では存在していなかった「2」の剰余が出現している。

図5は改竄のない場合であり、「2」の剰余が存在しなかったことから  $A / (A + C) = 1$  であるが、仮に、図6において前記の範囲を領域指定すると、 $A = 4$ 、 $C = 6$  であるために  $A / (A + C) = 0.4$  となり、 $A / (A + C)$  は大きく減少する。

即ち、実施形態1の場合よりも厳格な基準で改竄の有無を正確に判定できることになる。

#### 【0048】

尚、この実施形態では、データ処理装置側で画素ブロックの輝度平均値の整数値が「4」の倍数となるように規則性をもたせ、改竄判定装置の除算部25で除数を「4」に設定して、その除算結果の剰余の中央値：「2」の出現状態を判定要素としているが、必ずしも「4」とする必要性はなく、それより大きい整数倍に設定してもよい。

その場合、例えば、設定値が「5」のときには「0」から「5」までの整数の中央値として「2」と「3」があり、一般に奇数が設定されたときには2つの中央値が考えられるが、奇数を設定したときには双方の剰余を中央値としてカウント数：Cを求める。

何故なら、設定値を「5」のとしたときには、改竄が行われないう限り、剰余として「2」と「3」が出現する確率が極めて小さく、それより大きい奇数の場合には更に確率が小さくなるからである。

#### 【0049】

##### 【実施形態4】

以上の実施形態1、2、3では、データ処理装置と改竄判定装置を機能ブロック図（図1、図2、図3）で表したように、各装置をハードウェアで構成することを前提としているが、各装置が実行する機能はマイクロコンピュータ回路（以下、「マイコン回路」という）によってソフトウェア的に実行させることも可能である。

#### 【0050】

先ず、図7はマイコン回路40で構成したデータ処理装置の構成を示す。

ここで、マイコン回路40はCPU41、ROM42、RAM43、I/Oポート44からなる通常のシステム回路を有しているが、ROM42には、システム制御プログラムと共に、図1のデータ分離部、平均値演算部3、画素輝度書換部4、R/W制御部5、データ合成部6及びエンコーダ部7が実行する機能手順に係るプログラムモジュールが格納されており、CPU41がRAM43を画像メモリ及びワークエリアとして利用しながら前記の各プログラムモジュールを実行するようになっている。

#### 【0051】

次に、このデータ処理装置のデータ処理手順を図9のフローチャートを参照しながら説明する。

但し、処理内容自体は上記の実施形態1で説明したデータ処理装置とほぼ同様であり、ここでは前記のプログラムモジュールが時系列的に順次実行される手順を中心に説明することとする。

先ず、I/Oポート44を介して外部から供給されるデジタル画像データを8×8画素ブロック単位で取り込んでRAM43にセーブし、輝度／色差データ分離モジュールを起動して輝度データと色差データを分離した後、その分離後のデータを再びRAM43にセーブする（S1～S3）。

そのセーブが完了すると、輝度平均の整数演算モジュールを起動させ、画素ブロックの各画素の輝度値  $L(i)$  [ $i=1\sim64$ ] を求め、更に画素ブロックの輝度平均値： $L_{av} (= \sum L(i) / 64)$  を求め、その平均値： $L_{av}$  を四捨五入して整数化した値： $L_{av}'$  を求める（S4

)。

そして、輝度データ書換えモジュールを起動させ、前記の整数化値： $L_{av'}$ が整数： $N$ の倍数である場合にはそのままとするが( $S5 \rightarrow S7$ )、 $N$ の倍数でない場合には、整数化値： $L_{av'}$ が $N$ の倍数となるように、画素ブロックの各画素の輝度データを最小の諧調変更幅( $+\Delta p$ 又は $-\Delta m$ )となる条件で書き換える( $S6$ )。

尚、ここでは「 $N$ 」として表現しているが、 $N$ は2又は4の何れか一方に設定されるものとする。

その結果、画素ブロックにはその平均輝度が $N$ の倍数であるという規則性が与えられたことになる。

#### 【0052】

前記の輝度データの操作が完了すると、輝度／色差データ合成モジュールを起動して輝度データと色差データを合成した後、J P E Gの符号化処理モジュールを起動して合成後の画素ブロックの画像データを符号化して圧縮し、その圧縮画像データをI/Oポート44から出力させる( $S7 \sim S9$ )。

以降、前記のステップS1からステップS9を繰り返すことにより、外部から供給される1フレーム分の画像データを画素ブロック単位で処理して出力させる( $S10 \rightarrow S1 \sim S10$ )。

そして、出力された符号化後の圧縮画像データは、一旦何等かの記憶手段に格納され、それを記憶媒体に記録して提供されるか、又は通信回線を介して提供先へ配信されることになる。

#### 【0053】

次に、図9はマイコン回路50で構成した改竄判定装置の構成を示す。

マイコン回路50はCPU51、ROM52、RAM53、I/Oポート54からなる通常のシステム回路を有しているが、ROM52には、システム制御プログラムと共に、図2又は図4のデコーダ部21、輝度データ分離部22、平均値演算部24、除算部25、書込制御部26、計数部32及び改竄判定部34が実行する機能手順に係るプログラムモジュールが格納されており、CPU51がRAM53を画像メモリ及びワークエリアとして利用しながら前記の各プログラムモジュールを実行するようになっている。

また、I/Oポート54には表示部55がインターフェイス56を介して接続されていると共に、領域設定部57からI/Oポート54を介して判定対象となる画像領域を指定できるようになっている。

#### 【0054】

次に、この改竄判定装置のデータ処理手順を図10のフローチャートを参照しながら説明する。

但し、処理内容自体は上記の実施形態1、2、3で説明した改竄判定装置とはほぼ同様であり、ここでは前記のプログラムモジュールが時系列的に順次実行される手順を中心に説明することとする。

尚、実施形態1と実施形態2、3で説明した改竄判定装置ではそれぞれ改竄判定基準が異なっているため、改竄判定に係る手順については個別に説明する。

#### 【0055】

先ず、I/Oポート54を介して外部から供給されるデジタル画像データを取り込んでRAM53に一旦セーブし、J P E Gの復号処理モジュールを起動して画像データを復号化し、その復号後の画像データをRAM53にセーブする( $S21, S22$ )。

但し、画像データの取り込みと復号化に際しては、J P E Gの符号化画像データでは直前の画素ブロックのDC係数を予測値とした差分値を符号化するため、少なくとも前後する2つの画素ブロックをRAM53にセーブさせて復号処理を行う。

#### 【0056】

次に、輝度／色差データ分離モジュールを起動して、復号化された画像データの輝度データを分離した後、その輝度データをRAM53にセーブする( $S23, S24$ )。

そして、輝度平均演算モジュールを起動し、画素ブロックの輝度平均値： $L_{avx}$ (= $\sum L_e(i)x/64$ )を演算し、その平均値： $L_{xav}$ を四捨五入して整数化した値： $L_{avx'}$ を求

める (S25)。

また、前記の整数化値:  $L_{avx}'$  が求まると、除算モジュールを起動して  $L_{avx}'/N$  を求め、その除算結果の剰余だけを RAM 53 にセーブする (S26, S27)。

但し、除数の  $N$  は前記のデータ処理装置側で適用した値 (この実施形態では「2」又は「4」の何れか一方) を適用する。

#### 【0057】

以降、以上のステップ S21 からステップ S27 の手順は、1 フレーム分の画像データについての処理が完了するまで繰り返して実行され、その結果、1 フレーム分の画像ブロックに係る前記剰余値が RAM 53 にセーブされた状態となる。

この改竄判定装置では、この段階で判定手順 (S29) を行うことになるが、その判定手順は  $N$  の設定の仕方及び判定基準の設定の仕方によって異なる。

従って、それぞれの判定手順を以下の (1) ~ (3) に分けて具体的に説明する。

#### 【0058】

(1) この判定手順は、上記の実施形態 1 で説明した改竄判定装置が採用している判定基準に対応しており、データ処理装置及びこの改竄判定装置での符号化・復号化処理が理想的なものであって、データ処理装置側で各画素ブロックに与えた規則性が符号化・復号化過程で損なわれないことを前提としている。

この判定手順は図 11 のフローチャートに示される。

まず、判定モジュールが起動されると、CPU 51 は RAM 53 の全ての剰余値を走査し、その中に「0」以外の値が含まれているか否かを確認する (S41)。

そして、1 つでも「0」以外の値が含まれていれば「改竄あり」と判定し、全てが「0」であれば「改竄なし」と判定する (S41→S42, S43)。

また、その判定結果は I/O ポート 54 からインターフェイス 56 を介して表示部 55 へ出力される (S44)。

#### 【0059】

(2) この判定手順は上記の実施形態 2 で説明した改竄判定装置が採用している判定基準に対応しており、データ処理装置及びこの改竄判定装置での符号化・復号化過程で各画素ブロックに与えた規則性が損なわれていることを考慮したものである。

この判定手順は図 12 のフローチャートに示される。

まず、領域設定部 57 から判定対象とする画像領域の指定が行われると、判定閾値設定モジュールが起動し、閾値:  $Z1$  が設定される (S51, S52)。

この閾値:  $Z1$  は、予め実験的に確認されている符号化・復号化過程での前記の規則性の損壊度合い及び予想される改竄領域の大きさと領域設定部 57 による指定領域のサイズとの相対的關係をパラメータとして最適値に設定される。

具体的には、閾値設定モジュールは前記のパラメータを用いて閾値:  $Z1$  を選択するためのテーブルを有しており、領域設定部 57 からの領域指定情報に基づいて閾値:  $Z1$  を設定する。

#### 【0060】

次に、剰余値カウントモジュールが起動され、RAM 53 の全ての剰余値を走査して「0」の剰余値の個数:  $A$  と、「0」以外の剰余値の個数:  $B$  をそれぞれカウントする (S53)。

そして、そのカウントが完了すると判定モジュールが起動され、 $A/(A+B)$  を演算してその演算結果を  $Z1$  と比較し、 $A/(A+B) \leq Z1$  の条件が成立していれば「改竄あり」と判定し、逆の場合には「改竄なし」と判定する (S54→S55, S56)。

また、前記 (1) の場合と同様に、その判定結果は表示部 55 へ出力される (S57)。

#### 【0061】

(3) この判定手順は上記の実施形態 3 で説明した改竄判定装置が採用している判定基準に対応しており、前記 (2) の場合と同様に、データ処理装置及びこの改竄判定装置での符号化・復号化過程で各画素ブロックに与えた規則性が損なわれていることを考慮したものである。

先ず、領域設定部 57 から判定対象とする画像領域の指定が行われると、判定閾値設定モジュールが起動し、閾値：Z2 が設定される (S61, S62)。

この場合の閾値：Z2 が、予め実験的に確認されている符号化・復号化過程での前記の規則性の損壊度合い及び予想される改竄領域の大きさと領域設定部 57 による指定領域のサイズとの相対的關係をパラメータとして求められることは前記 (2) と同様であるが、次のステップ S63 に示すように剰余値の内のカウント対象が異なるため、その閾値：Z2 は前記 (2) の閾値：Z1 より大きい値として設定される。

#### 【0062】

次に、剰余値カウントモジュールが起動され、RAM 53 の全ての剰余値を走査して「0」の剰余値の個数：A と、「0」～「N」の中央値である剰余値の個数：C をそれぞれカウントする (S63)。

この場合、「N」が 4 であるため、剰余値「2」の個数が C としてカウントされることになる。

そして、そのカウントが完了すると判定モジュールが起動され、 $A / (A + C)$  を演算してその演算結果を Z2 と比較し、 $A / (A + C) \leq Z2$  の条件が成立していれば「改竄あり」と判定し、逆の場合には「改竄なし」と判定する (S64→S65, S66)。

また、前記 (1), (2) の場合と同様に、その判定結果は表示部 55 へ出力される (S67)。

#### 【0063】

ここで、図 10 のフローチャートに戻って、前記の (1) ～ (3) の各判定手順で出力される判定結果は表示部 55 で表示される (S30)。

そして、この改竄判定装置では、入力画像データを復号化しており、また前記 (1) では改竄された画像領域が特定でき、前記 (2) 及び (3) では領域指定情報が得られていることから、判定結果の表示に際しては、復号化した再生画像を表示部 55 に表示させておき、その表示画面上で改竄領域を示すことや指定領域に係る改竄の有無を示すことも可能である。

また、この改竄判定装置では、判定基準選択モードを設けておき、前記の (1) ～ (3) の各判定手順を選択的に実行させるようにしてもよい。

尚、前記のデータ処理装置側と改竄判定装置側にそれぞれ持たせる各プログラムは、記録媒体に格納した提供方式だけでなく、インターネット等の通信回線を介して提供してもよく、それぞれ適当なシステムを用いてマイクロコンピュータ回路に実装させることができる。

#### 【0064】

##### 【その他】

以上の実施形態では、8×8 画素の画素ブロックを単位として処理することとしているが、原理的に画素ブロックのサイズは問わず、16×16 画素等の画素ブロックについても有効であることは当然である。

また、JPEG 方式の符号化・復号化処理がなされることを前提として説明したが、MPEG 方式で符号化・復号化がなされる動画像データについても適用できる。

その場合、P ピクチャや B ピクチャについてはフレーム間の相関を利用した圧縮が行われるために画素ブロックに与えた規則性がかなり大きく損なわれることになるが、I ピクチャに関してはフレーム内圧縮だけが行われるために大きな損壊はなく、I ピクチャの画素ブロックにのみ前記の規則性を与えるようにすればよい。

#### 【0065】

尚、上記の各実施形態 1, 2, 3 の改竄判定装置では画素ブロック単位で画素の輝度データをセーブさせるための画像メモリ 23 を用いているが、改竄判定装置では画像データの書き換えを行わないため、輝度データから各画素の輝度値を逐次検出しながら平均値演算を行うようにしてもよく、その場合には画像メモリ 23 は不要になる。

##### 【図面の簡単な説明】

#### 【0066】

【図 1】本発明のデータ処理装置の実施形態（実施形態 1 乃至 3 で共通）に係る機能ブロック図である。

【図 2】本発明の改竄判定装置（実施形態 1）に係る機能ブロック図である。

【図 3】実施形態 1 の改竄判定装置における除算部での除算結果の剰余の出現態様を示す図である。

【図 4】本発明の改竄判定装置（実施形態 2 及び実施形態 3）に係る機能ブロック図である。

【図 5】実施形態 2 において、改竄がなされていない場合に、改竄判定装置の除算部による除算結果の剰余の出現状態の一例を示す図である。

【図 6】実施形態 3 において、改竄がなされている場合に、改竄判定装置の除算部による除算結果の剰余の出現状態の一例を示す図である。

【図 7】本発明の実施形態 4 に係るデータ処理装置（マイコン回路で構成した場合）のシステム回路図である。

【図 8】本発明の実施形態 4 に係る改竄判定装置（マイコン回路で構成した場合）のシステム回路図である。

【図 9】実施形態 4 に係るデータ処理装置のデータ処理手順を示すフローチャートである。

【図 10】実施形態 4 に係る改竄判定装置の全体的なデータ処理手順を示すフローチャートである。

【図 11】改竄判定手順（1）を詳細に表したフローチャートである。

【図 12】改竄判定手順（2）を詳細に表したフローチャートである。

【図 13】改竄判定手順（3）を詳細に表したフローチャートである。

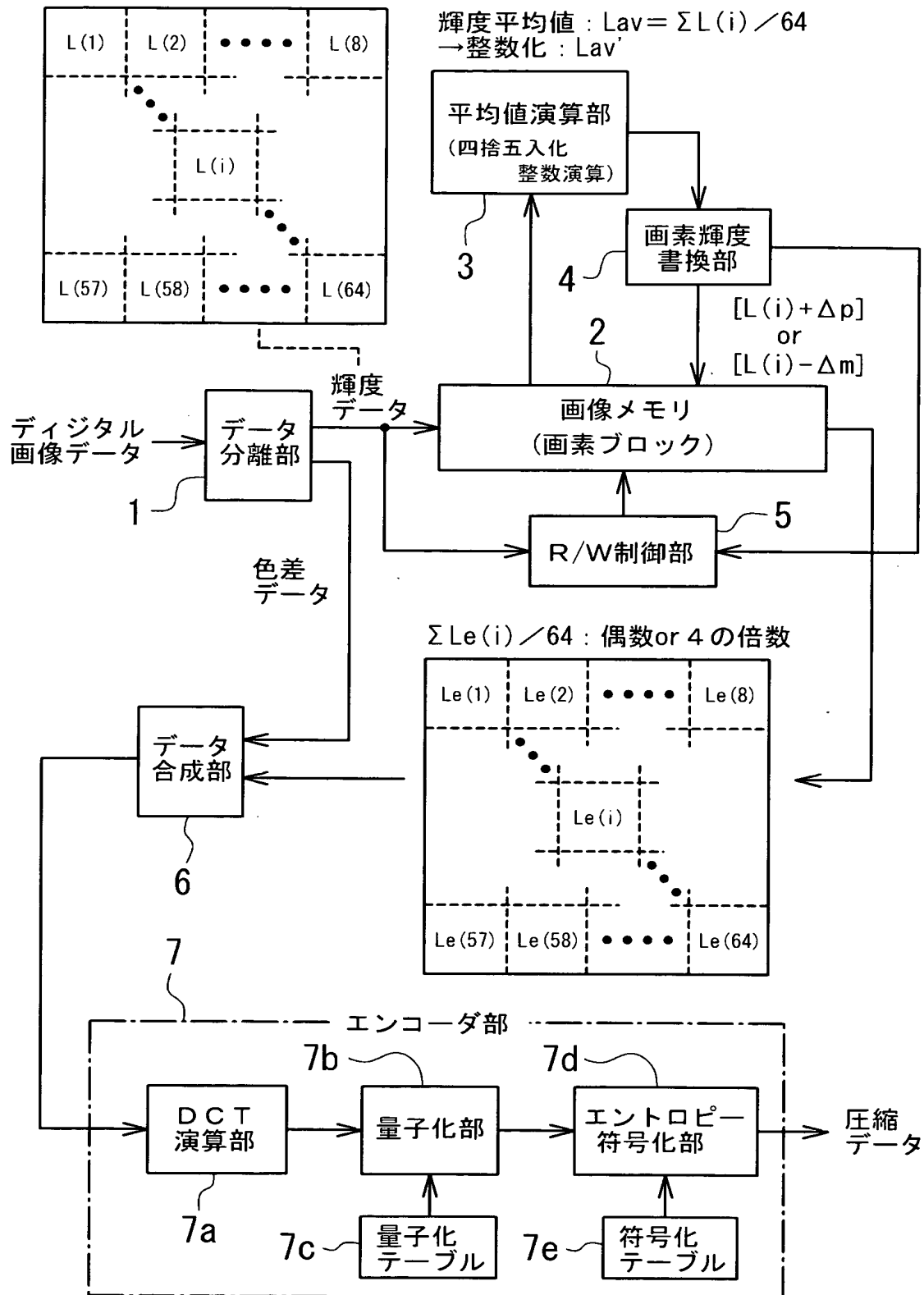
【符号の説明】

【0067】

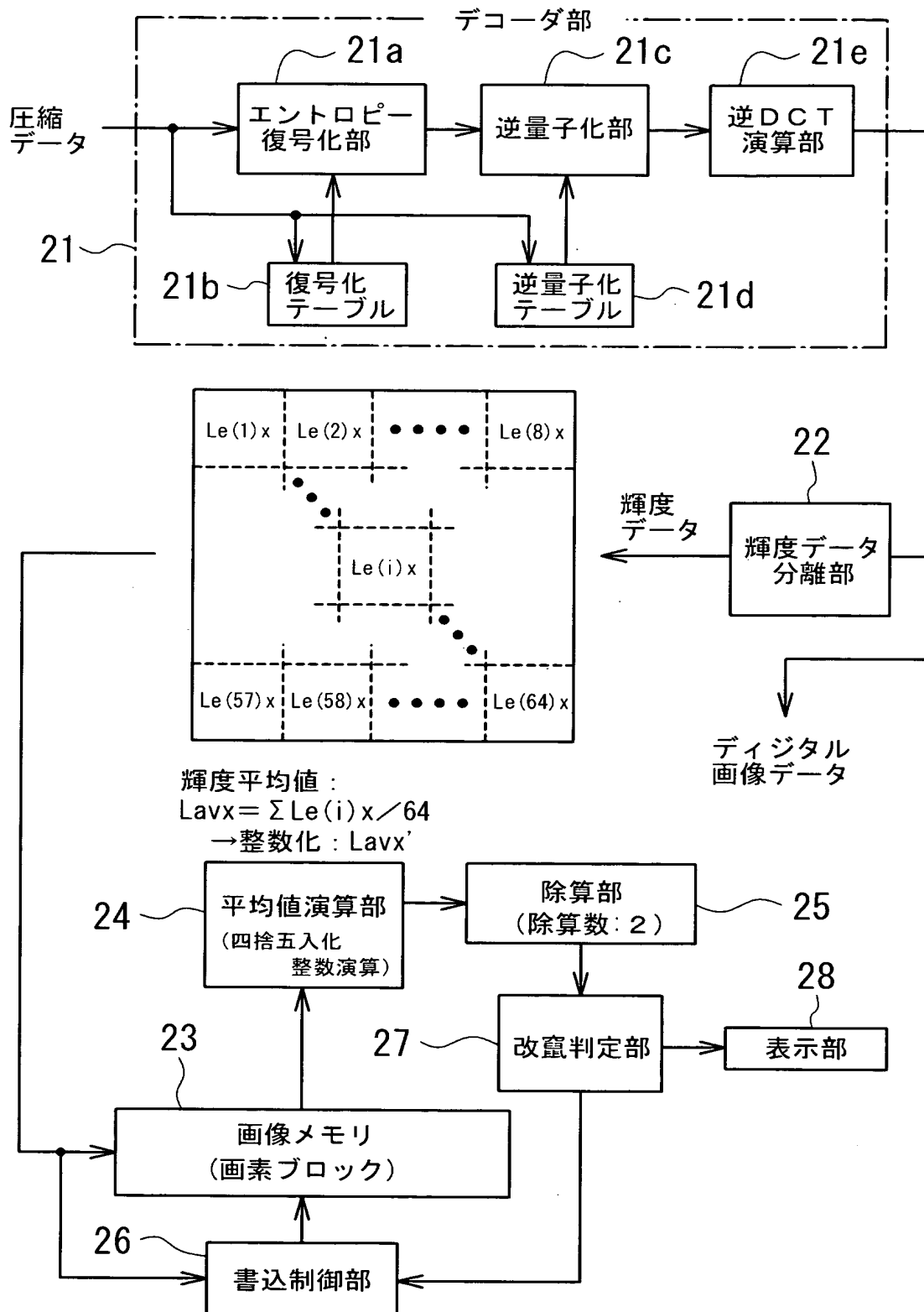
1…データ分離部、2, 23…画像メモリ、3, 24…平均値演算部、4…画素輝度書換部、5…R/W制御部、6…データ合成部、7…エンコーダ部、7a…DCT演算部、7b…量子化部、7c…量子化テーブル、7d…エントロピー符号化部、7e…符号化テーブル、21…デコーダ部、21a…エントロピー復号化部、21b…復号化テーブル、21c…逆量子化部、21d…逆量子化テーブル、21e…逆DCT演算部、22…輝度データ分離部、25…除算部、26…書込制御部、27, 34…改竄判定部、28, 55…表示部、31…剰余メモリ、32…計数部、33, 57…領域設定部、40, 50…マイコン回路、41, 51…CPU、42, 52…ROM、43, 53…RAM、44, 54…I/Oポート、56…インターフェイス。

【書類名】 図面

【図 1】

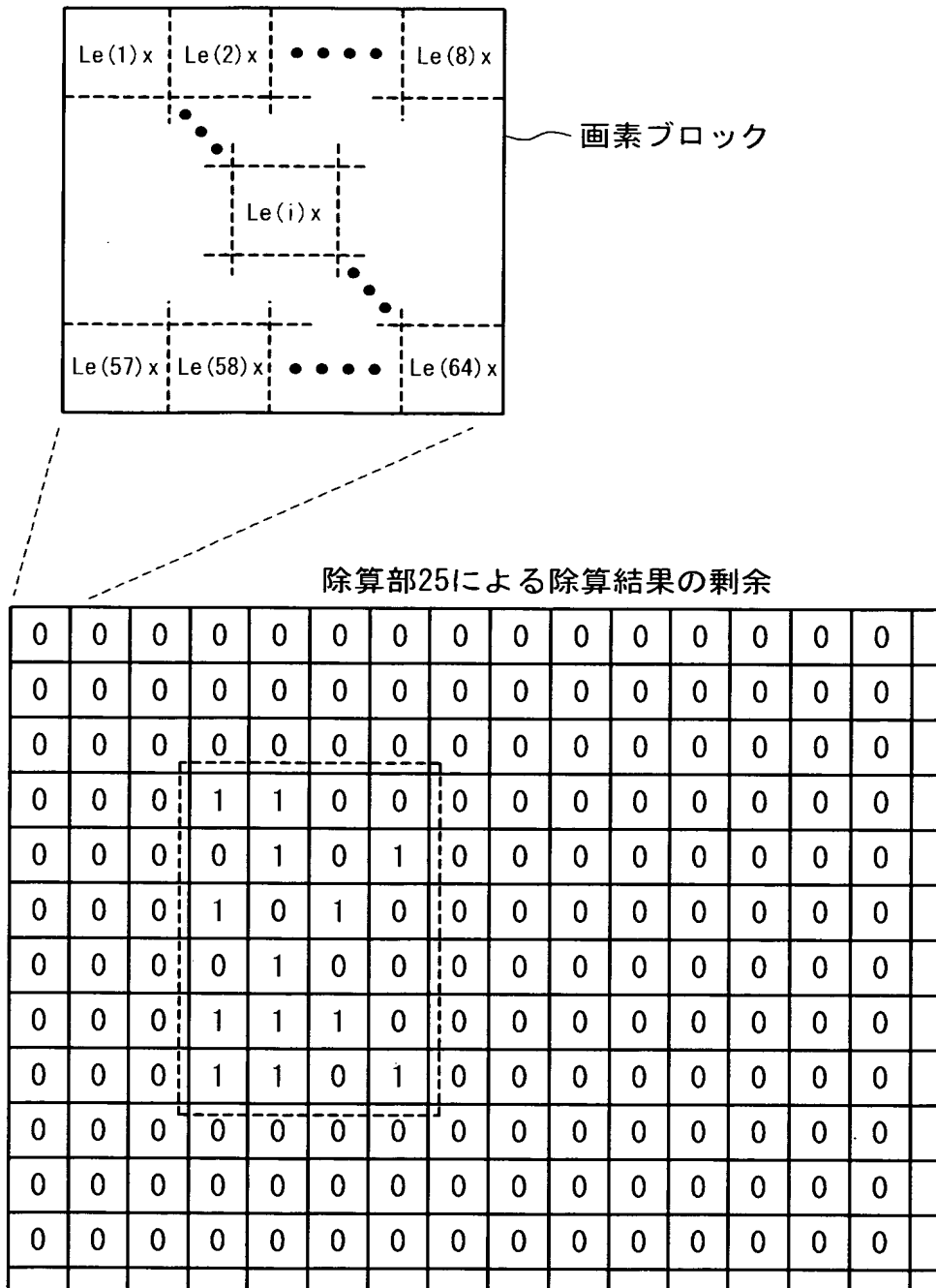


【図 2】

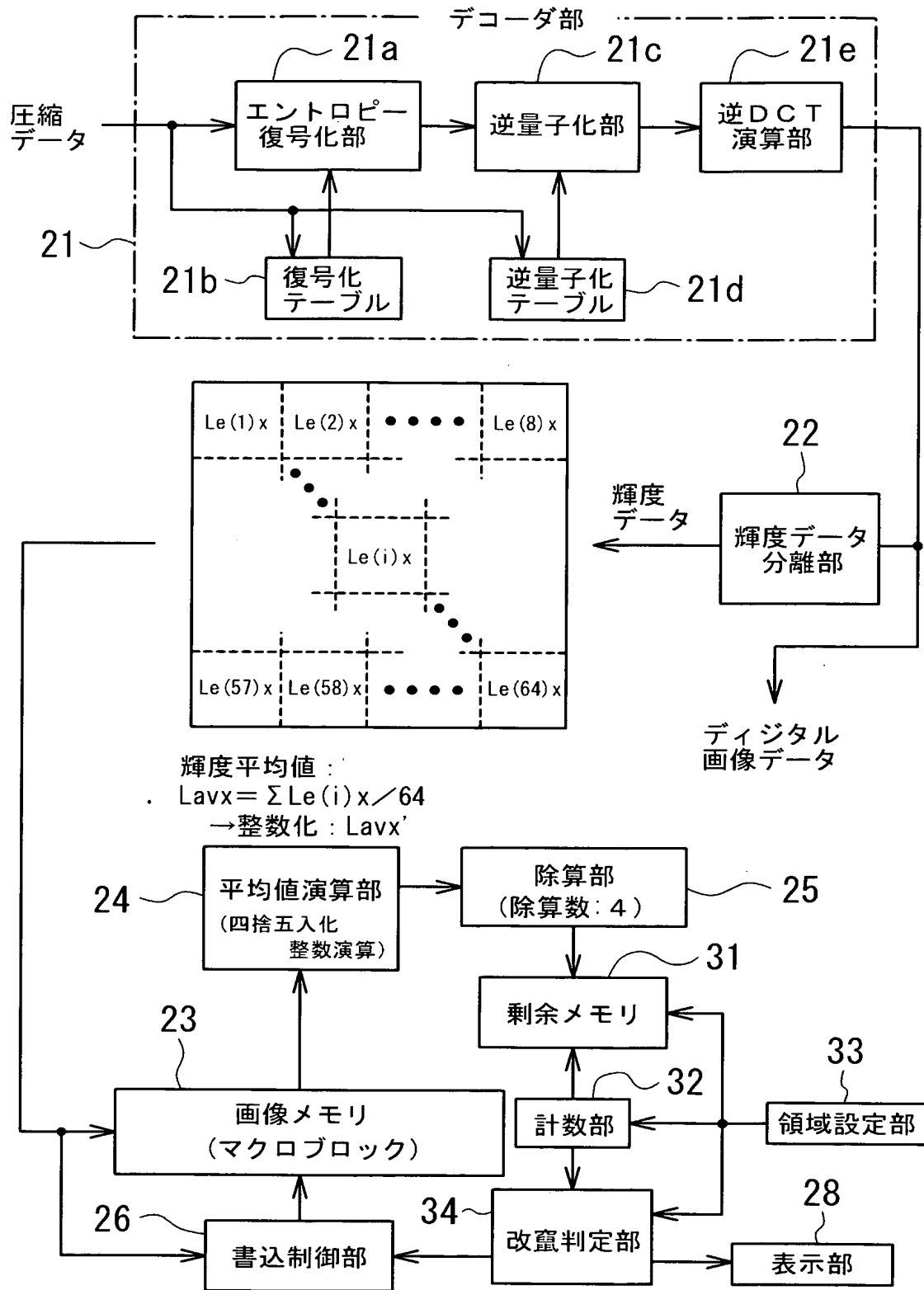




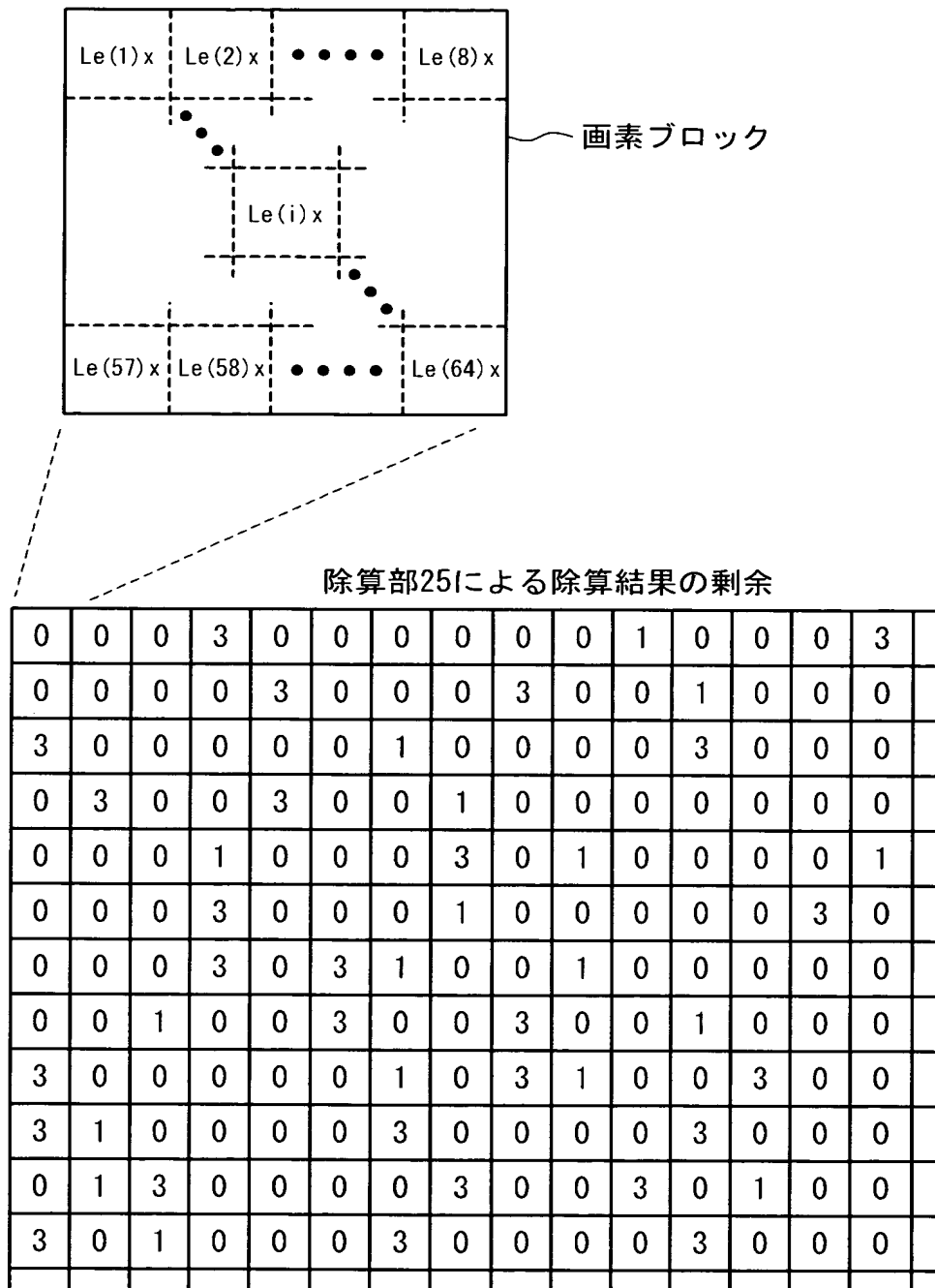
【図 3】



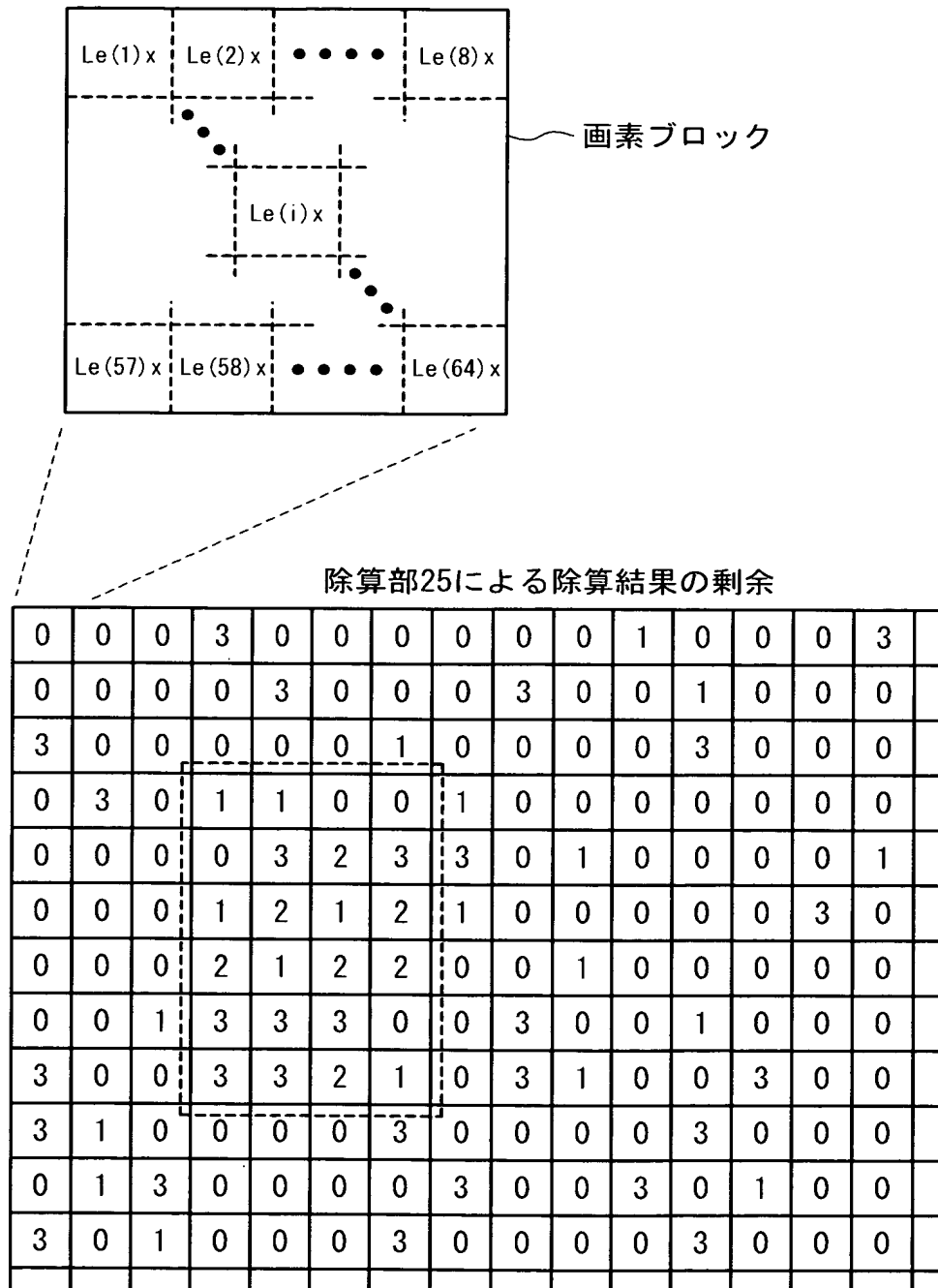
【図 4】



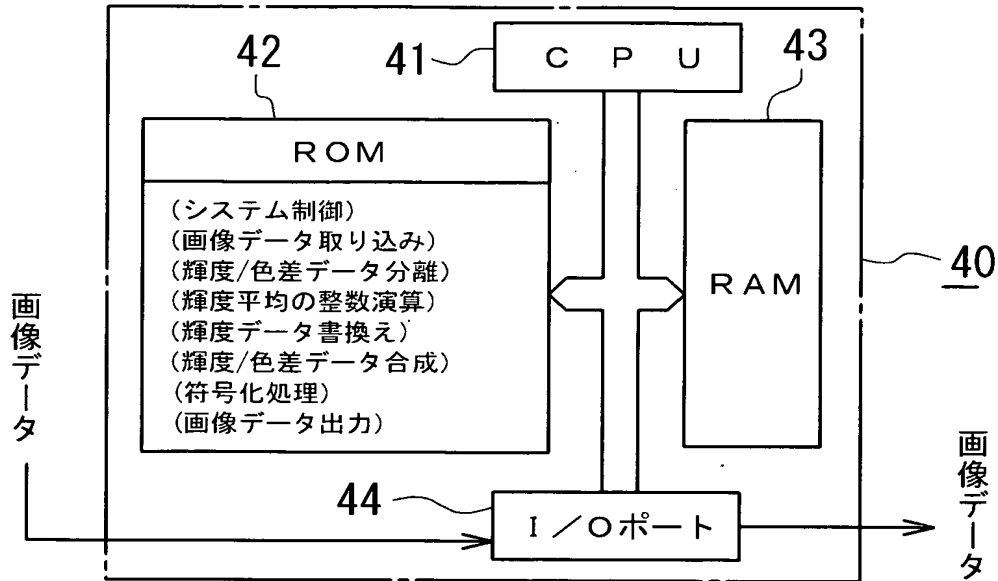
【図 5】



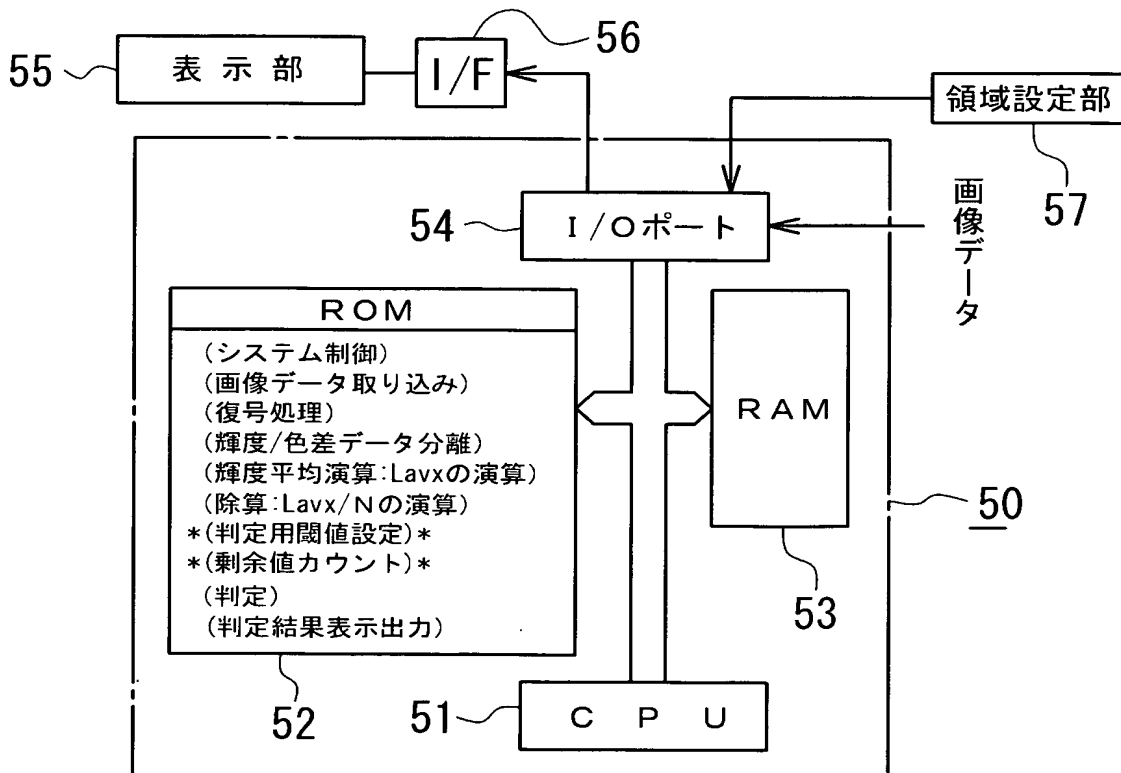
【図 6】



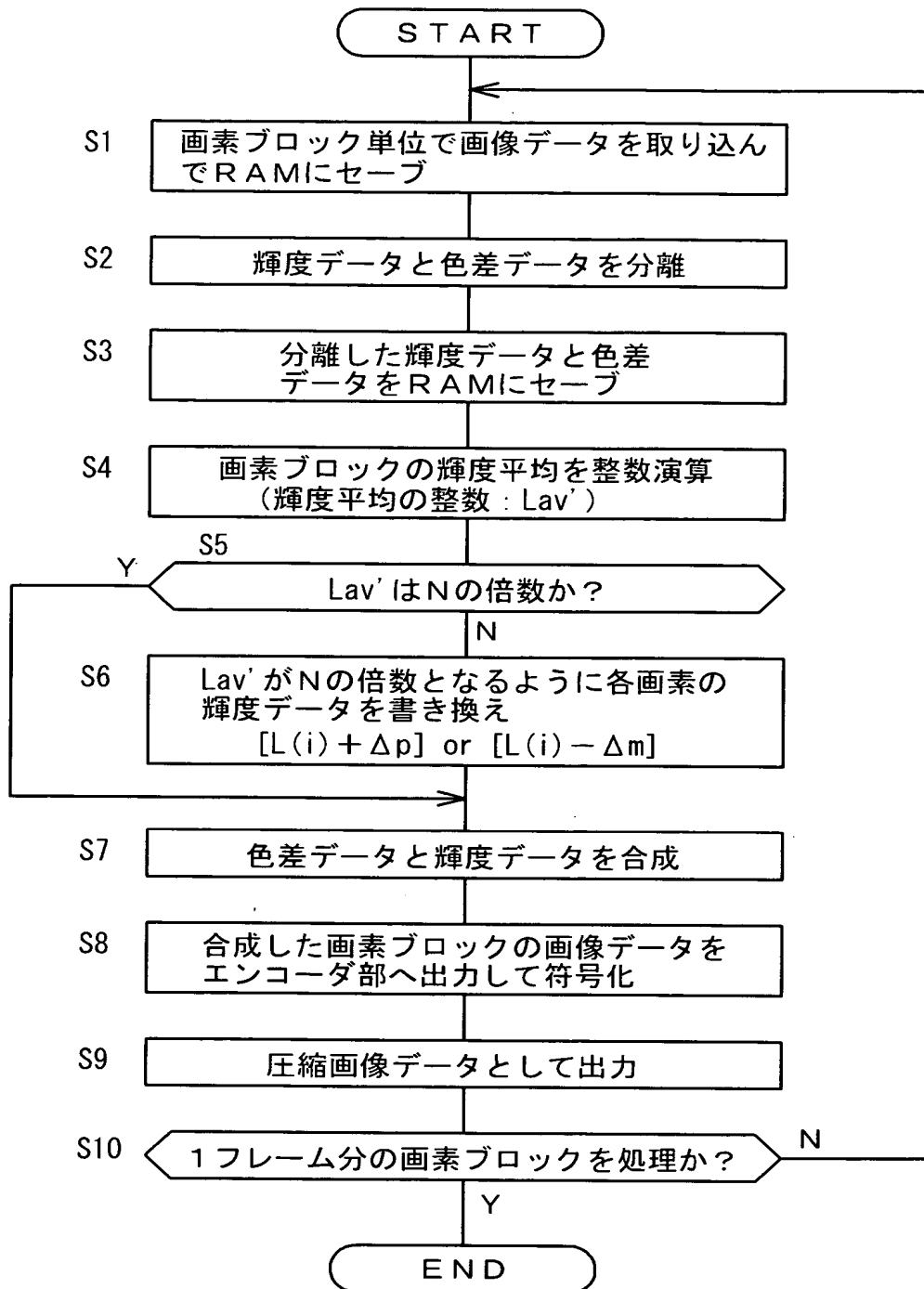
【図 7】



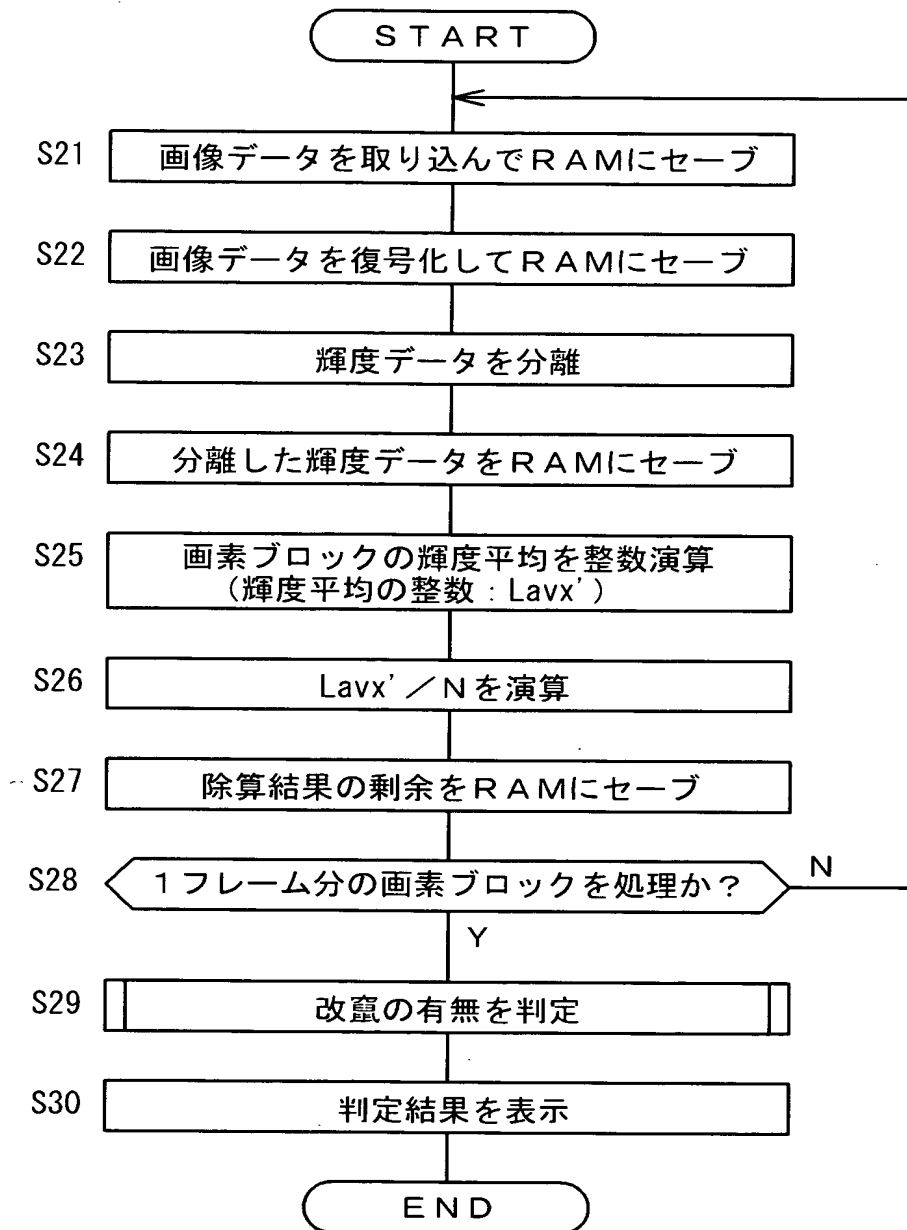
【図 8】



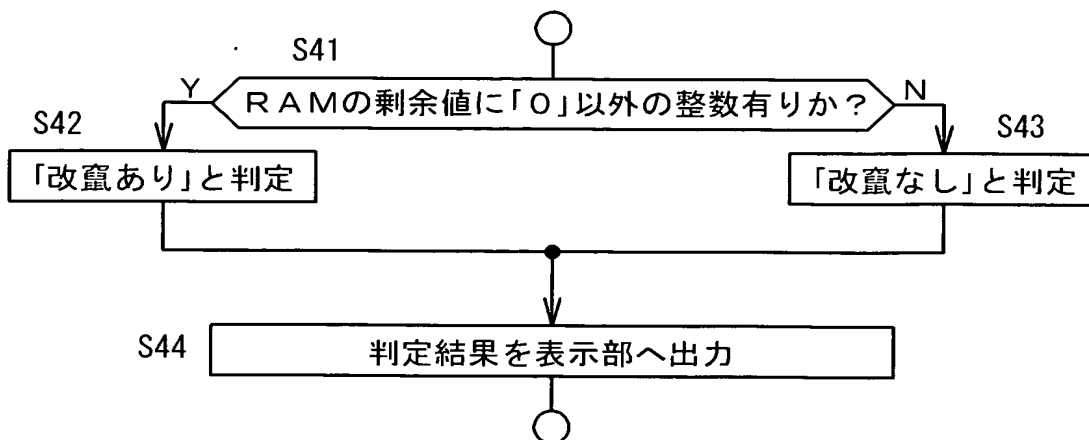
【図 9】



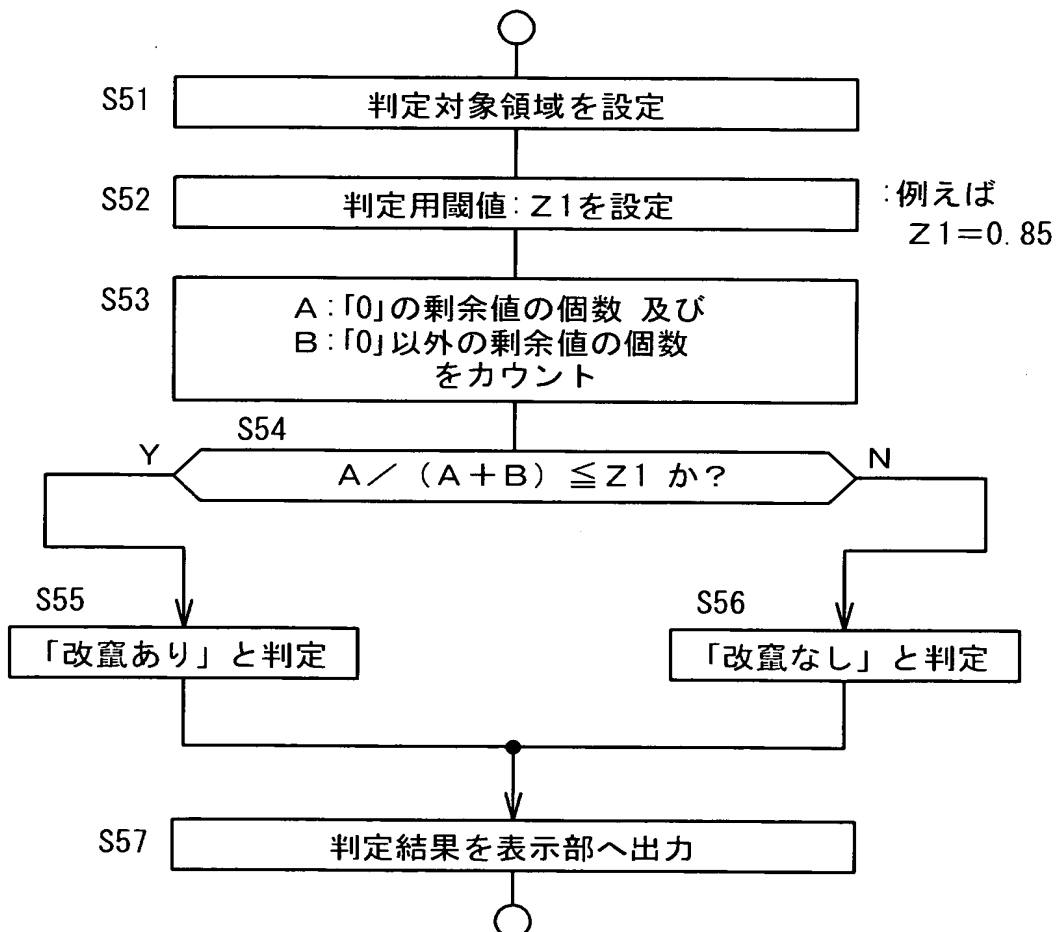
【図 10】



【図 11】

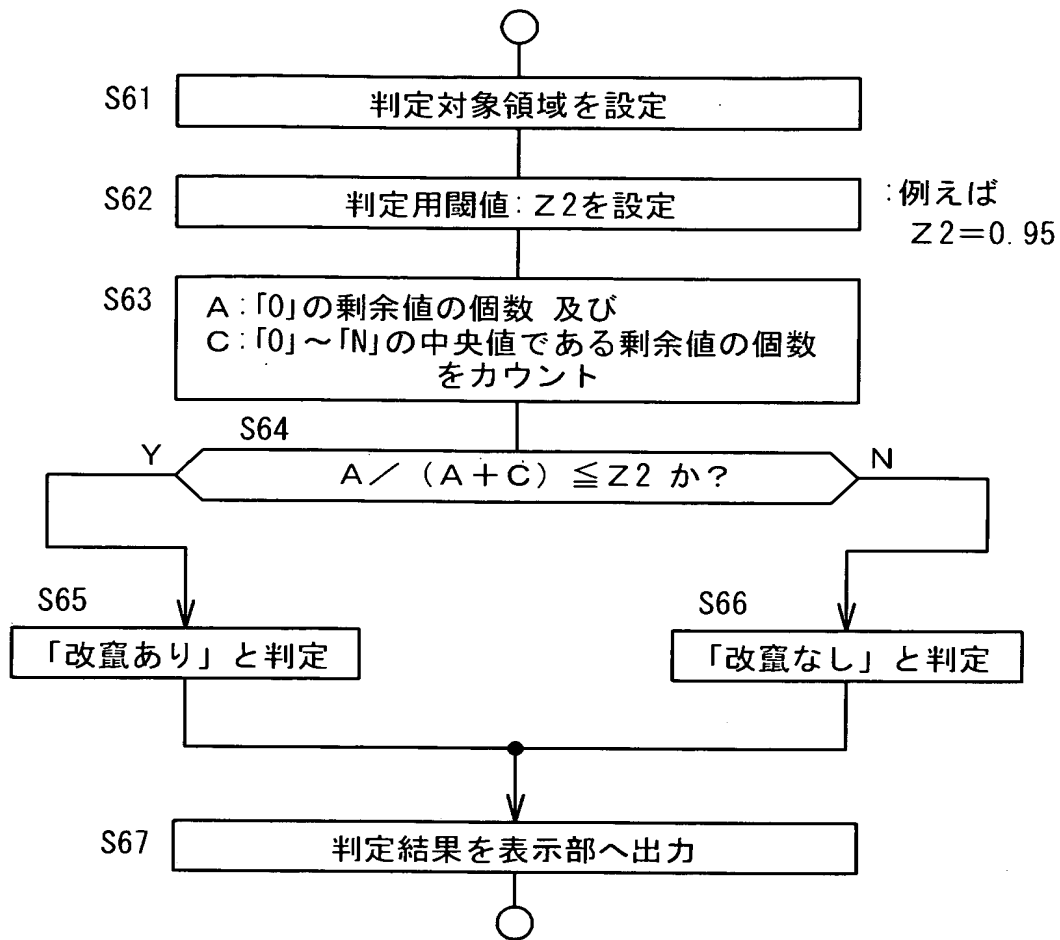


【図 12】





【図 13】



**【書類名】 要約書****【要約】**

**【課題】** 画像データに対して、直交変換を含む符号化前に改竄判定用の秘匿的情報を付与しても正確な改竄判定が可能になるシステムを提供する。

**【解決手段】** データ処理装置側では、画素ブロック単位でその輝度平均値が $N (= 4)$ の倍数となるように各画素の輝度データを最小諧調ステップ数で書き換え、その画像データを符号化する。改竄判定装置側では、平均値演算部 24 で画素ブロックの輝度平均の整数化値を求め、その値を除算部 25 が除数 4 で除算し、その剰余を剰余メモリ 31 にセーブする。領域設定部 33 で画像領域を設定し、計数部 32 で設定領域内の剰余 0 の数：A と剰余 2 (0 ～ N の中央値) の数：C を求める。データ処理装置側のエンコーダと改竄判定部のデコーダの特性及び設定領域サイズ等をパラメータとして閾値：Z2 を設定し、 $A / (A + C) \leq Z2$  が成立すれば「改竄あり」と判定する。

**【選択図】** 図 4

特願 2 0 0 3 - 3 5 6 7 9 1

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 4 3 2 9 ]

1. 変更年月日

1 9 9 0 年 8 月 8 日

[変更理由]

新規登録

住 所

神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地

氏 名

日本ビクター株式会社